UNITED STATES PATENT APPLICATION

FOR

CONTROLLED DELIVERY OF DIGITAL CONTENT IN A SYSTEM FOR DIGITAL CONTENT ACCESS CONTROL

INVENTOR:

Eduard K. de Jong, a citizen of the Netherlands

ASSIGNED TO:

Sun Microsystems, Inc., a Delaware Corporation

PREPARED BY:

THELEN, REID & PRIEST LLP
P.O. BOX 640640
SAN JOSE, CA 95164-0640
TELEPHONE: (408) 292-5800
FAX: (408) 287-8040

Attorney Docket Number: SUN-P8727

Client Docket Number: P8727

SPECIFICATION

TITLE OF INVENTION

CONTROLLED DELIVERY OF DIGITAL CONTENT IN A SYSTEM FOR DIGITAL CONTENT ACCESS CONTROL

Cross Reference to Related Applications

[0001] This application is a Continuation-In-Part of the following co-pending United States Patent Applications in the name of the inventors hereof (and others) and bearing the serial numbers, filing dates and titles shown below.

Serial No.	Filing Date	Title
10/243,858	September 13, 2002	System for Digital Content Access Control
10/243,355	September 13, 2002	Accessing for Digital Content Access Control
10/243,218	September 13, 2002	Synchronizing for Digital Content Access Control
10/243,474	September 13, 2002	Repositing for Digital Content Access Control
10/243,287	September 13, 2002	Provisioning for Digital Content Access Control

This application is related to the following:

[0002] U.S. Patent Application Serial No. _____, filed September 19 in the name of inventor Eduard K. de Jong, entitled "Accessing for Controlled Delivery of Digital Content in a System for Digital Content Access Control", Attorney Docket No. SUN-040105, commonly assigned herewith.

[0003] U.S. Patent Application Serial No. 10/014,893, filed October 29, 2001 in the name of inventors Eduard de Jong, Moshe Levy and Albert Leung, entitled "User Access Control to Distributed Resources on a Data Communications Network", Attorney Docket No. SUN-P6992, commonly assigned herewith.

[0004] U.S. Patent Application Serial No. 10/040,270, filed October 29, 2001 in the name of inventors Eduard de Jong, Moshe Levy and Albert Leung, entitled "Enhanced Privacy Protection in Identification in a Data Communications Network", Attorney Docket No. SUN-P6990, commonly assigned herewith.

[0005] U.S. Patent Application Serial No. 10/014,823, filed October 29, 2001 in the name of inventors Eduard de Jong, Moshe Levy and Albert Leung, entitled "Enhanced Quality of Identification in a Data Communications Network", Attorney Docket No. SUN-P6991, commonly assigned herewith.

[0006] U.S. Patent Application Serial No. 10/014,934, filed October 29, 2001 in the name of inventors Eduard de Jong, Moshe Levy and Albert Leung, entitled "Portability and Privacy with Data Communications Network Browsing", Attorney Docket No. SUN-P7007, commonly assigned herewith.

[0007] U.S. Patent Application Serial No. 10/033,373, filed October 29, 2001 in the name of inventors Eduard de Jong, Moshe Levy and Albert Leung, entitled "Managing Identification in a Data Communications Network", Attorney Docket No. SUN-P7014, commonly assigned herewith.

[0008] U.S. Patent Application Serial No. 10/040,293, filed October 29, 2001 in the name of inventors Eduard de Jong, Moshe Levy and Albert Leung, entitled "Privacy and Identification in a Data Communications Network", Attorney Docket No. SUN-P7015, commonly assigned herewith.

FIELD OF THE INVENTION

[0009] The present invention relates to the field of computer science. More particularly, the present invention relates to controlled delivery of digital content in a system for digital content access control.

BACKGROUND OF THE INVENTION

[0010] Figure 1 is a block diagram that illustrates a typical mechanism for digital content access control. A mobile phone operator 100 includes a portal 150 by which one or more mobile phones 125-140 communicate with one or more content producers 105-120 via a network 175

such as the Internet. Mobile phone operator 100 also includes a product catalog 145 that includes a description of digital content 155-170 stored by digital content producers 105-170. A particular digital content producer controls access to digital content stored by the digital content producer. Thus, authenticators 180-195 control access to digital content 155-170, respectively.

[0011] A user desiring access to digital content 155-170 stored by a digital content producer 105-120 uses a mobile phone 125-140 to issue an access request to a particular digital content producer 105-120. The digital content producer 105-195 authenticates the user making the request. The authentication typically includes prompting the user for a username and a password if the username and password is not included with the initial access request. Upon successful user authentication, the digital content producer 105-120 may grant access to the digital content 155-170. Alternatively, the digital content producer 105-120 may issue a token that may be presented at a later time and redeemed in exchange for access to the digital content.

[0012] Unfortunately, the bandwidth available for communications with digital content producers 105-120 is relatively limited. If the available bandwidth is exceeded, a user may be denied service. This problem is exacerbated as the number of users increases.

[0013] Accordingly, a need exists in the prior art for a digital content access control solution that requires relatively less communication with digital content producers. A further need exists for such a solution that is relatively secure. Yet another need exists for such a solution that is relatively scaleable.

SUMMARY OF THE INVENTION

[0014] A content provisioner controls access to digital content by receiving a digital content request comprising a request for digital content, creating an authenticated digital content request if a user associated with the digital content request is authorized to access the digital content, determining one or more delivery parameters identifying a target device to receive the digital content, and sending the authenticated digital content request including the one or more delivery parameters. A content repository validates the authenticated digital content request, determines a session key if the authenticated digital content request is valid, encrypts the digital content using the session key, and sends the encrypted digital content. Determining a session key includes determining a target key based at least in part on a target ID, and applying a cryptographic process to a first key based at least in part on the authenticated digital content request, together with the target key.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] The accompanying drawings, which are incorporated into and constitute a part of this specification, illustrate one or more embodiments of the present invention and, together with the detailed description, serve to explain the principles and implementations of the invention.

In the drawings:

FIG. 1 is a block diagram that illustrates a typical mechanism for digital content access control.

FIG. 2 is a block diagram of a computer system suitable for implementing aspects of the present invention.

FIG. 3 is a block diagram that illustrates a system for digital content access control in accordance with one embodiment of the present invention.

FIG. 4 is a block diagram that illustrates a system for digital content access control with a requesting user device and a receiving user device in accordance with one embodiment of the present invention.

FIG. 5 is a block diagram that illustrates a system for digital content access control using a portal in accordance with one embodiment of the present invention.

FIG. 6A is a diagram that illustrates a universal resource locator (URL).

FIG. 6B is a diagram that illustrates a tokenized URL having an appended token in accordance with one embodiment of the present invention.

FIG. 6C is a diagram that illustrates a tokenized URL having an appended parameterized token in accordance with one embodiment of the present invention.

FIG. 6D is a diagram that illustrates a tokenized URL for use in accessing digital content at a content repository having an access domain dedicated to accepting tokenized URLs in accordance with one embodiment of the present invention.

FIG. 6E is a diagram that illustrates a tokenized URL for use in accessing digital content at a content repository having an access domain dedicated to accepting tokenized URLs in accordance with one embodiment of the present invention.

FIG. 6F is a diagram that illustrates a tokenized URL for use in accessing digital content at a particular content locker of a content repository having an access domain dedicated to accepting tokenized URLs in accordance with one embodiment of the present invention.

FIG. 7A is a diagram that illustrates a tokenized URL for use in accessing a content repository having an access domain capable of performing functions in addition to accepting tokenized URLs in accordance with one embodiment of the present invention.

FIG. 7B is a diagram that illustrates a tokenized URL for use in accessing digital content at a content repository having an access domain capable of performing functions in addition to accepting tokenized URLs in accordance with one embodiment of the present invention.

FIG. 7C is a diagram that illustrates a tokenized URL for use in accessing digital content at a particular content locker of a content repository having an access domain capable of performing functions in addition to accepting tokenized URLs in accordance with one embodiment of the present invention.

FIG. 8 is a block diagram that illustrates a system for program code module access control in accordance with one embodiment of the present invention.

FIG. 9 is a block diagram that illustrates a system for audio file access control in accordance with one embodiment of the present invention.

FIG. 10 is a block diagram that illustrates a system for XML (Extensible Markup Language) document access control in accordance with one embodiment of the present invention.

FIG. 11 is a block diagram that illustrates a system for Web page access control in accordance with one embodiment of the present invention.

FIG. 12 is a block diagram that illustrates a system for digital content access control having one or more content repositories associated with a content provisioner in accordance with one embodiment of the present invention.

FIG. 13 is a block diagram that illustrates a system for digital content access control having one or more content provisioners associated with a content repository in accordance with one embodiment of the present invention.

FIG. 14 is a block diagram that illustrates a system for digital content access control having one or more content provisioners and content repositories associated with a synchronizer in accordance with one embodiment of the present invention.

FIG. 15 is a block diagram that illustrates a system for digital content access control where a secure user device activates deactivated tokens issued by a content provisioner and uses the activated tokens to access digital content stored by a content repository in accordance with one embodiment of the present invention.

FIG. 16 is a block diagram that illustrates a system for digital content access control where a secure user device activates deactivated tokens issued by a content provisioner and uses the activated tokens to access digital content stored by a content repository in accordance with one embodiment of the present invention.

FIG. 17 is a block diagram that illustrates token pool allocation and synchronization in a system for digital content access control in accordance with one embodiment of the present invention.

FIG. 18A is a diagram that illustrates a token in accordance with one embodiment of the present invention.

FIG. 18B is a diagram that illustrates a token that comprises a chain ID in accordance with one embodiment of the present invention.

FIG. 18C is a diagram that illustrates a token that comprises a chain ID and a maximum length in accordance with one embodiment of the present invention.

FIG. 18D is a diagram that illustrates a token that comprises a chain ID and an identifier in a series in accordance with one embodiment of the present invention.

FIG. 18E is a diagram that illustrates a token that comprises a chain ID and an offset representing an identifier in a series in accordance with one embodiment of the present invention.

FIG. 18F is a diagram that illustrates a token that comprises a token type in accordance with one embodiment of the present invention.

FIG. 19 is a block diagram that illustrates creating a token chain by applying a cryptographic process to one or more identifiers in a series together with a token chain key in accordance with one embodiment of the present invention.

FIG. 20 is a block diagram that illustrates creating a token chain by applying a cryptographic process to a filler and one or more identifiers in a series together with a token chain key in accordance with one embodiment of the present invention.

FIG. 21 is a block diagram that illustrates creating a token chain using cryptographic one-way functions in accordance with one embodiment of the present invention.

FIG. 22 is a flow diagram that illustrates a method for creating and using a token pool formed by applying a cryptographic process to an identifier in a series together with a token chain key in accordance with one embodiment of the present invention.

FIG. 23 is a flow diagram that illustrates a method for creating and using a token pool formed by successive applications of a cryptographic one-way function in accordance with one embodiment of the present invention.

FIG. 24 is a data flow diagram that illustrates communicating token pool information from a synchronizer in accordance with one embodiment of the present invention.

FIG. 25 is a block diagram that illustrates allocating tokens from a token pool comprising one or more token chains created using a cryptographic one-way function in accordance with one embodiment of the present invention.

FIG. 26 is a block diagram that illustrates a token pool having a current token pool for current token redemptions, a retired token pool for tokens that have been available for redemption for a predetermined time and a buffered token pool for future token redemptions in accordance with one embodiment of the present invention.

FIG. 27 is a detailed block diagram that illustrates initialization of a system for digital content access control in accordance with one embodiment of the present invention.

FIG. 28 is a flow diagram that illustrates a method for digital content access control from the perspective of a user device in accordance with one embodiment of the present invention.

FIG. 29 is a flow diagram that illustrates a method for digital content access control from the perspective of a secure user device in accordance with one embodiment of the present invention.

FIG. 30 is a flow diagram that illustrates a method for initializing a digital content producer in accordance with one embodiment of the present invention.

FIG. 31 is a flow diagram that illustrates a method for initializing a digital content provisioner in accordance with one embodiment of the present invention.

FIG. 32 is a flow diagram that illustrates a method for content repository initialization in accordance with one embodiment of the present invention.

FIG. 33 is a flow diagram that illustrates a method for synchronizer initialization in accordance with one embodiment of the present invention.

FIG. 34 is a detailed block diagram that illustrates a system for digital content access control in accordance with one embodiment of the present invention.

FIG. 35 is a flow diagram that illustrates a method for digital content access control from the perspective of a user device in accordance with one embodiment of the present invention.

FIG. 36 is a flow diagram that illustrates a method for digital content access control from the perspective of a user device in accordance with one embodiment of the present invention.

FIG. 37 is a flow diagram that illustrates a method for digital content access control from the perspective of a secure user device in accordance with one embodiment of the present invention.

FIG. 38 is a flow diagram that illustrates a method for digital content access control from the perspective of a digital content provisioner in accordance with one embodiment of the present invention.

FIG. 39 is a flow diagram that illustrates a method for digital content access control from the perspective of a digital content provisioner in accordance with one embodiment of the present invention.

FIG. 40 is a flow diagram that illustrates a method for creating an authenticated digital content request in accordance with one embodiment of the present invention.

FIG. 41 is a flow diagram that illustrates a method for digital content access control from the perspective of a digital content repository in accordance with one embodiment of the present invention.

FIG. 42 is a flow diagram that illustrates a method for validating an authenticated digital content request using a pre-computed token pool comprising multi-use tokens in accordance with one embodiment of the present invention.

FIG. 43 is a block diagram that illustrates a sliding token offset window for use in dynamic token computation in accordance with one embodiment of the present invention.

FIG. 44 is a flow diagram that illustrates a method for validating an authenticated digital content request by dynamically computing tokens using a sliding token offset window in accordance with one embodiment of the present invention.

FIG. 45 is a flow diagram that illustrates a method for validating an authenticated digital content request by dynamically computing tokens using a sliding token offset window having a dynamic size in accordance with one embodiment of the present invention.

FIG. 46 is a flow diagram that illustrates a method for validating an authenticated digital content request by dynamically computing tokens using a sliding token offset window having a static size in accordance with one embodiment of the present invention.

FIG. 47 is a flow diagram that illustrates a method for updating an offset in accordance with one embodiment of the present invention.

FIG. 48 is a flow diagram that illustrates a method for validating an authenticated digital content request using a pre-computed token pool comprising single-use tokens computed using a cryptographic one-way function in accordance with one embodiment of the present invention.

FIG. 49 is a flow diagram that illustrates a method for validating an authenticated digital content request using a pre-computed token pool comprising single-use tokens computed using a cryptographic one-way function and ordered according to token redemption status in accordance with one embodiment of the present invention.

FIG. 50 is a flow diagram that illustrates a method for validating an authenticated digital content request by dynamically computing single-use tokens using a cryptographic one-way function in accordance with one embodiment of the present invention.

FIG. 51 is a flow diagram that illustrates a method for digital content access control from the perspective of a synchronizer in accordance with one embodiment of the present invention.

FIG. 52 is a block diagram that illustrates controlled delivery of digital content to a target device via a user device in a system for digital content access control in accordance with one embodiment of the present invention.

FIG. 53 is a flow diagram that illustrates controlled delivery of digital content to a target device via a user device in a system for digital content access control in accordance with one embodiment of the present invention.

FIG. 54 is a block diagram that illustrates controlled delivery of digital content to a target device in a system for digital content access control in accordance with one embodiment of the present invention.

FIG. 55 is a flow diagram that illustrates controlled delivery of digital content to a target device in a system for digital content access control in accordance with one embodiment of the present invention.

FIG. 56A is a high level data flow diagram that illustrates encrypting digital content for controlled delivery of digital content to a target device in a system for digital content access control in accordance with one embodiment of the present invention.

FIG. 56B is a high level data flow diagram that illustrates decrypting digital content for controlled delivery of digital content to a target device in a system for digital content access control in accordance with one embodiment of the present invention.

FIG. 57A is a low level data flow diagram that illustrates encrypting digital content for controlled delivery of digital content to a target device in a system for digital content access control in accordance with one embodiment of the present invention.

FIG. 57B is a low level data flow diagram that illustrates decrypting digital content for controlled delivery of digital content to a target device in a system for digital content access control in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION

[0016] Embodiments of the present invention are described herein in the context of controlled delivery of digital content in a system for digital content access control. Those of ordinary skill in the art will realize that the following detailed description of the present invention is illustrative only and is not intended to be in any way limiting. Other embodiments of the present invention will readily suggest themselves to such skilled persons having the benefit of this disclosure. Reference will now be made in detail to implementations of the present invention as illustrated in the accompanying drawings. The same reference indicators will be used throughout the drawings and the following detailed description to refer to the same or like parts.

[0017] In the interest of clarity, not all of the routine features of the implementations described herein are shown and described. It will, of course, be appreciated that in the development of any such actual implementation, numerous implementation-specific decisions must be made in order to achieve the developer's specific goals, such as compliance with application- and business-related constraints, and that these specific goals will vary from one implementation to another and from one developer to another. Moreover, it will be appreciated that such a development effort might be complex and time-consuming, but would nevertheless be a routine undertaking of engineering for those of ordinary skill in the art having the benefit of this disclosure.

[0018] In accordance with one embodiment of the present invention, the components, process steps, and/or data structures may be implemented using various types of operating systems (OS), computing platforms, firmware, computer programs, computer languages, and/or general-purpose machines. The method can be run as a programmed process running on processing circuitry. The processing circuitry can take the form of numerous combinations of processors and operating systems, or a stand-alone device. The process can be implemented as instructions executed by such hardware, hardware alone, or any combination thereof. The software may be stored on a program storage device readable by a machine.

[0019] In addition, those of ordinary skill in the art will recognize that devices of a less general purpose nature, such as hardwired devices, field programmable logic devices (FPLDs), including field programmable gate arrays (FPGAs) and complex programmable logic devices (CPLDs), application specific integrated circuits (ASICs), or the like, may also be used without departing from the scope and spirit of the inventive concepts disclosed herein.

[0020] In accordance with one embodiment of the present invention, the method may be implemented on a data processing computer such as a personal computer, workstation computer, mainframe computer, or high performance server running an OS such as Solaris® available from Sun Microsystems, Inc. of Santa Clara, California, Microsoft® Windows® XP and Windows® 2000, available form Microsoft Corporation of Redmond, Washington, or various versions of the Unix operating system such as Linux available from a number of vendors. The method may also be implemented on a multiple-processor system, or in a computing environment including various peripherals such as input devices, output devices, displays, pointing devices, memories,

storage devices, media interfaces for transferring data to and from the processor(s), and the like. In addition, such a computer system or computing environment may be networked locally, or over the Internet.

[0021] In the context of the present invention, the term "network" comprises local area networks, wide area networks, the Internet, cable television systems, telephone systems, wireless telecommunications systems, fiber optic networks, ATM networks, frame relay networks, satellite communications systems, and the like. Such networks are well known in the art and consequently are not further described here.

[0022] In the context of the present invention, the term "randomized" describes the result of a random or pseudo-random number generation process. A "randomized process" describes the application of such a result to a process. Methods of generating random and pseudo-random numbers are known by those skilled in the relevant art.

[0023] In the context of the present invention, the term "identifier" describes one or more numbers, characters, symbols, or the like. More generally, an "identifier" describes any entity that can be represented by one or more bits.

[0024] In the context of the present invention, the term "authenticator" describes an identifier for use in obtaining access to digital content associated with the authenticator.

[0025] In the context of the present invention, the term "token" describes an authenticator comprising a cryptogram.

[0026] In the context of the present invention, the term "token key" describes a cryptographic key based at least in part on a token.

[0027] In the context of the present invention, the term "cryptographic one-way function" describes any cryptographic process that produces an output based upon an input, such that it is computationally infeasible to compute the input based upon the output. Exemplary cryptographic one-way functions comprise the MD4 algorithm and the MD5 algorithm. The MD4 algorithm is described in R. Rivest, *The MD4 Message Digest Algorithm*, Request for Comments (RFC) 1320, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992. The MD5 algorithm is described in Rivest. R. *The MD5 Message-Digest Algorithm*, Request for Comments (RFC) 1321, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992.

[0028] In the context of the present invention, the term "encryption" describes the application of one or more cryptographic processes to one or more data items.

[0029] In the context of the present invention, the term "delivery parameter" describes any value used to determine the destination or target device to which digital content is delivered, pre-processing to be performed before delivery of the digital content, post-processing to be performed after delivery of the digital content, or a mechanism used to deliver the digital

content. By way of example, a delivery parameter may comprise one or more of the following: a target device identifier (target ID) that indicates a target device to receive digital content, a transport means identifier that indicates the transport means used to deliver digital content to the target device, a master key, an encryption algorithm identifier, an encryption algorithm parameter value, or an identifier for a digital content protection mechanism used to create a session key or a target key,

[0030] Figure 2 depicts a block diagram of a computer system 200 suitable for implementing aspects of the present invention. As shown in FIG. 2, computer system 200 comprises a bus 202 which interconnects major subsystems such as a central processor 204, a system memory 206 (typically RAM), an input/output (I/O) controller 208, an external device such as a display screen 210 via display adapter 212, serial ports 214 and 216, a keyboard 218, a fixed disk drive 220, a floppy disk drive 222 operative to receive a floppy disk 224, and a CD-ROM player 226 operative to receive a CD-ROM 228. Many other devices can be connected, such as a pointing device 230 (e.g., a mouse) connected via serial port 214 and a modem 232 connected via serial port 216. Modem 232 may provide a direct connection to a server via a telephone link or to the Internet via a POP (point of presence). Alternatively, a network interface adapter 234 may be used to interface to a local or wide area network using any network interface system known to those skilled in the art (e.g., Ethernet, xDSL, AppleTalk™).

[0031] Many other devices or subsystems (not shown) may be connected in a similar manner. Also, it is not necessary for all of the devices shown in FIG. 2 to be present to practice the present invention, as discussed below. Furthermore, the devices and subsystems may be

interconnected in different ways from that shown in FIG. 2. The operation of a computer system such as that shown in FIG. 2 is readily known in the art and is not discussed in detail in this application, so as not to overcomplicate the present discussion. Code to implement the present invention may be operably disposed in system memory 206 or stored on storage media such as fixed disk 220, floppy disk 224 or CD-ROM 228.

[0032] Turning now to FIG. 3, a block diagram that illustrates a system for digital content access control in accordance with one embodiment of the present invention is presented. System 370 may comprise at least one user device 300, at least one content provisioner 315 and at least one content repository 320 that communicate via a network 310. System 370 may also comprise a synchronizer 325 in communication with the content provisioner 315 and the content repository 320. User device 300 is configured to send a digital content request 350 and receive digital content 365 in response to the digital content request 350.

[0033] User device 300 may be any device configured to render digital content to a user 305. By way of example, user device 300 may comprise a personal digital assistant (PDA), a personal computer (PC), a mobile phone, a digital audio player (such as an MP3 player), a game console, a server computer in communication with a user display, or the like. According to another embodiment of the present invention, user device 300 comprises a secure portable device such as a Java Card™ technology-enabled device, or the like. Java Card™ technology is described in Chen, Z. *Java Card™ Technology for Smart Cards – Architecture and Programmer's Guide*, Boston, Addison-Wesley, 2000.

[0034] According to one embodiment of the present invention, user device 300 comprises a CDMA technology-enabled smart card. CDMA technology-enabled smart cards are described in *Smart Card Stage I Description*, Version 1.1, CDMA Development Group - Smart Card Team Document (May 22, 1996).

[0035] According to another embodiment of the present invention, user device 300 comprises a SIM (Subscriber Identity Module card) card. The term "SIM card" describes the smart card used in GSM (Global System for Mobile Communications) mobile telephones. The SIM comprises the subscriber's personal cryptographic identity key and other information such as the current location of the phone and an address book of frequently called numbers. The SIM is described in *Digital cellular telecommunications system (phase 2+); Specification of the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface*, ETSI, GSM 11.11 version 7.4.0, Release 1998.

[0036] According to another embodiment of the present invention, user device 300 comprises a WIM (Wireless Interface Module). A WIM is a smart card in a WAP (Wireless Application Protocol) phone. It is described in *Wireless Identity Module Part: Security*, WAP-260-WIM-20010712-a , Wireless Application Protocol Forum, July 12, 2001.

[0037] According to another embodiment of the present invention, user device 300 comprises a USIM (Universal Subscriber Identity Module). A USIM is a smart card for a 3GPP (3rd Generation Partnership Project) mobile phone. It is described in *3rd Generation Partnership*

Project; Technical Specification Terminals; USIM and IC card requirements, Release 4, 3GPP TS 21.111 V4.0.0 (2001-03).

[0038] According to another embodiment of the present invention, user device 300 comprises a UIM (User Identity Module). A UIM is a smart card for a 3GPP Project 2 (3GPP2) mobile phone. The term "R-UIM" is used when the smart card is removable. A UIM is a super set of the SIM and allows CDMA (Code Division Multiple Access)-based cellular subscribers to roam across geographic and device boundaries. The R-UIM is described in a specification issued by the 3rd Generation Partnership Project 2 (3GPP2) and entitled 3rd Generation Partnership Project 2; Removable User Identity Module (R-UIM) for cdma2000 Spread Spectrum Systems, 3GPP2 C.S0023-0, June 9, 2000.

[0039] The above description regarding various mobile phone technologies is not intended to be limiting in any way. Those of ordinary skill in the art will recognize that other user devices may be used.

[0040] Referring again to FIG. 3, content provisioner 315 is configured to receive a digital content request 350 and return an authenticated digital content request 355 in response to the received digital content request 350. Content provisioner 315 may comprise a content rights database 330 to store an association between one or more users and a description of the digital content that the one or more users are authorized to access. Content provisioner 315 may also comprise a provisioner manager 335 in communication with the content rights database 330. Provisioner manager 335 is configured to receive a digital content request 350 and communicate

with content rights database 330 to determine whether the user 305 that made the request 350 is authorized to access the digital content associated with the request 350. Provisioner manager 335 may comprise an issuer 375 to issue a token for use in creating an authenticated digital content request 335. Alternatively, content provisioner 315 may comprise an issuer external to and in communication with a provisioner manager. Provisioner manager 335 is also configured to communicate with user device 300 to obtain user authentication data such as a password, PIN, biometric data or the like. If the user device 300 comprises a mobile phone, the user authentication data may also comprise a mobile phone subscriber ID, or the like. According to one embodiment of the present invention, the authenticated digital content request 355 comprises a cryptogram based at least in part on an identifier that describes the location of the digital content for which access is authorized. According to another embodiment of the present invention, the cryptogram comprises at least one token from a token pool associated with the location of the digital content for which access is authorized.

[0041] Content repository 320 is configured to receive an authenticated digital content request 360 and return digital content 365 corresponding to the authenticated digital content request 360. Content repository 320 may comprise a content database 340 to store digital content corresponding to at least one digital content description stored by at least one content provisioner 315. Content repository 320 also may comprise a repository manager 345 in communication with the content database 340. Repository manager 345 is configured to receive an authenticated digital content request 360, communicate with the content database 340 to determine whether the authenticated digital content request 360 is valid and return the digital content associated with the authenticated digital content request when the authenticated digital

content request is valid. Repository manager 345 may also comprise an acceptor 380 to accept a token and determine whether the access to the digital content associated with the authenticated digital content request is authorized based at least in part on the token. Alternatively, content repository 320 may comprise an acceptor external to and in communication with a repository manager 345.

[0042] Synchronizer 325 is configured to synchronize the information used by the content provisioner 315 to create authenticated digital content requests with the information used by content repository 320 to validate digital content requests. The authenticated digital content request information may comprise, by way of example, a token pool, information for use in generating a token pool, and the number of tokens released by the content provisioner 315. According to one embodiment of the present invention, the content provisioner 315 triggers the synchronization. According to another embodiment of the present invention, the content repository 320 triggers the synchronization. According to another embodiment of the present invention, the synchronization is triggered by the synchronizer, based at least in part on a predetermined schedule.

[0043] According to one embodiment of the present invention, a content provisioner comprises a synchronizer (not shown in FIG. 3). According to another embodiment of the present invention, a content repository comprises a synchronizer (not shown in FIG. 3).

[0044] In operation, user device 300 sends a digital content request 350 to content provisioner 315. According to one embodiment of the present invention, the digital content

request 350 may be based at least in part on information received from content provisioner 315. This information may comprise, by way of example, an indication of one or more services available to user 305. Provisioner manager 335 in content provisioner 315 receives the digital content request 350 and communicates with content rights database 330 to determine whether the user 305 that made the request 350 is authorized to access the digital content associated with the request 350. Provisioner manager 335 may also communicate with user device 300 to obtain user authentication data such as a password, PIN, biometric data or the like. If the user device 300 comprises a mobile phone, the user authentication data may also comprise a mobile phone subscriber ID, or the like. If the user 305 that made the request 350 is authorized to access the digital content 365 associated with the digital content request 350, issuer 335 issues a token and provisioner manager 335 sends an authenticated digital content request 355 based at least in part on the token to user device 300. User device 300 receives the authenticated digital content request 355 and then sends the authenticated digital content request 360 to a content repository 320. Repository manager 345 in content repository 320 receives the authenticated digital content request 320 and communicates with acceptor 380 and content database 340 to determine whether the authenticated digital content request 360 is valid. If the authenticated digital content request 360 is valid, repository manager 345 returns the digital content 365 associated with the authenticated digital content request 360. User device 300 receives the digital content 365 for use by user 305.

[0045] Turning now to FIG. 4, a block diagram that illustrates a system for digital content access control with a requesting user device and a receiving user device in accordance with one

embodiment of the present invention is presented. Figure 4 is similar to FIG. 3, except that FIG. 4 illustrates both a requesting user device 400 and a receiving user device 402.

[0046] Requesting user device 400 may be any device configured to accept user input and communicate over a communications network 410. Receiving user device 402 may be any device configured to render digital content to a user 405. By way of example, user device 402 may comprise a PDA, a PC, a mobile phone, a digital audio player (such as an MP3 player), a game console, a server computer in communication with a user display, or the like.

[0047] In operation, requesting user device 400 communicates with content provisioner 415 to obtain an authenticated digital content request 455. The authenticated digital content request 455 may comprise one or more delivery parameters that indicate a receiving user device to receive digital content associated with the authenticated digital content request 455. Alternatively, the authenticated digital content request 455 may be used to obtain delivery information. Requesting user device 400 sends the authenticated digital content request 460 to a content repository 420. Repository manager 445 in content repository 420 receives the authenticated digital content request 420 and communicates with acceptor 480 and content database 440 to determine whether the authenticated digital content request 460 is valid. If the authenticated digital content request 460 is valid, repository manager 445 sends the digital content 465 associated with the authenticated digital content request 460 to receiving device 402.

[0048] According to one embodiment of the present invention, requesting user device 400 comprises a user device having a relatively rich user interface such as a mobile phone or the like

and receiving user device 402 comprises a user device having a relatively limited user interface such as an MP3 (MPEG Audio Layer-3) player or the like.

[0049] Turning now to FIG. 5, a block diagram that illustrates a system for digital content access control using a portal in accordance with one embodiment of the present invention is presented. Figure 5 is similar to FIG. 3, except that in FIG. 5, user device 500 communicates with content repository 520 via a portal operator 515 that comprises at least one content provisioner 535. Whereas in FIG. 3, user device 300 communicates with content repository 320 directly via network 310.

[0050] In operation, user device 500 sends a digital content request 560 to portal 530 operated by portal operator 515. Portal 530 receives the digital content request 560 and communicates with provisioner manager 545 in content provisioner 535. Portal 530 may also communicate with user device 500 to obtain user authentication data such as a password, PIN, biometric data or the like. If the user device 500 comprises a mobile phone, the user authentication data may also comprise a mobile phone subscriber ID, or the like. Provisioner manager 545 receives the digital content request 560 and communicates with content rights database 540 to determine whether the user 505 that made the request 560 is authorized to access the digital content associated with the request 560. If the user 505 that made the request 560 is authorized to access the digital content associated with the request 560, issuer 585 issues an authenticator such as a token or the like and provisioner manager 545 sends an authenticated digital content request 565 based at least in part on the authenticator to content repository 520. Repository manager 555 in content repository 520 receives the authenticated digital content

request 565 and communicates with acceptor 580 and content database 550 to determine whether the authenticated digital content request 565 is valid. The authenticated digital content request 565 is valid if the digital content specified by the authenticated digital content request is associated with the authenticator portion of the authenticated digital content request. If the authenticated digital content request 565 is valid, repository manager 555 returns the digital content 570 associated with the authenticated digital content request 565. Portal operator 515 receives the digital content 570 and sends the digital content 575 to user device 500. User device 500 receives the digital content 575 for use by user 505. Alternatively, repository manager 555 may return the digital content 570 directly to user device 500 instead of routing the digital content through the portal operator 515. The delivery method may be based at least in part on information from the authenticated digital content request.

[0051] According to embodiments of the present invention, a token authenticates a specification (such as a Universal Resource Locator (URL)) of protected digital content. Validation of a token comprises determining whether the token authenticates a specification of digital content for which access is requested. These concepts are described in more detail below with reference to FIGS. 6A-6F and FIGS. 7A-7C.

[0052] Figure 6A is a diagram that illustrates a URL. Content domain indicator 602 specifies the host name of a Web server. Content directory indicator 604 specifies a directory at content domain 602 and accessed via delivery scheme 600 where the digital content specified by content item indicator 606 is stored. Exemplary delivery schemes comprise HTTP (Hypertext Transfer Protocol) and FTP (File Transfer Protocol).

[0053] Figures 6B-6F and 7A-7C are diagrams that illustrate tokenized URLs for use in accessing digital content stored at a content repository in accordance with embodiments of the present invention. Figure 6B illustrates a tokenized URL having an appended token. Figure 6C illustrates a tokenized URL having an appended parameterized token. Figure 6D illustrates using a tokenized URL to provide relatively fine-grained access control for digital content stored by a content repository having an access domain dedicated to accepting tokenized URLs, while FIG. 6F illustrates using a tokenized URL to provide relatively coarse-grained access control for digital content stored by a content repository having an access domain dedicated to accepting tokenized URLs. Similarly, FIG. 7A illustrates using a tokenized URL to provide relatively fine-grained access control for digital content stored by a content repository having an access domain capable of performing functions in addition to accepting tokenized URLs, while FIG. 7C illustrates using a tokenized URL to provide relatively coarse-grained access control for digital content stored by a content repository having an access domain capable of performing functions in addition to accepting tokenized URLs. Figures 6B-6F and 7A-7C are discussed in more detail below.

[0054] FIG. 6B is a diagram that illustrates a tokenized URL having an appended token in accordance with one embodiment of the present invention. Access domain indicator 612 in combination with delivery scheme indicator 610 specifies the URL of a content repository. Content directory indicator 614 specifies the pathname of a directory for at least one digital content item. Content item indicator 616 specifies a pathname for digital content located within content directory 614 at access domain 612 for which access is requested and controlled by the

token 618. Token indicator 618 specifies a token to use to access digital content within a context associated with the token. In this case, the context associated with the token comprises content item 616 within content directory 614 located at access domain 612. The token specifies a collection of digital content items made accessible by the token. Presenting token 618 entitles the presenter access to digital content 616 within content directory 614 at access domain 612.

[0055] FIG. 6C is a diagram that illustrates a tokenized URL having an appended parameterized token in accordance with one embodiment of the present invention. Figure 6C is similar to FIG. 6B except that a "Token=" named parameter or keyword 638 is used to delimit a token 640 in FIG. 6C.

[0056] Figure 6D is a diagram that illustrates a tokenized URL for use in accessing digital content at a content repository having an access domain dedicated to accepting tokenized URLs in accordance with one embodiment of the present invention. Access domain indicator 632 in combination with delivery scheme 650 specifies the URL of a content repository and token indicator 654 specifies a token to use to access digital content for a specific item located at access domain 632. The token specifies a single digital content item made accessible by the token, thus providing relatively fine-grained access control. Presenting token 654 entitles the presenter access to digital content at access domain 632. According to one embodiment of the present invention, delivery parameter indicator 656 is derived from a rights database (such as content rights database 540 of FIG. 5). Delivery parameter indicator 656 may indicate, by way of example, a cryptographic protection protocol, a destination address, a process to perform on the digital content before delivery, or any combination thereof. Delivery parameter indicator 656

may also comprise one or more content reference parameters. According to another embodiment of the present invention, delivery scheme indicator 650 specifies a specialized protocol that is private to a user device and particular digital content. By way of example, delivery scheme indicator 650 may indicate a special protocol for streaming media content.

[0057] Figure 6E is a diagram that illustrates a tokenized URL for use in accessing digital content at a content repository having an access domain dedicated to accepting tokenized URLs in accordance with one embodiment of the present invention. Access domain indicator 662 in combination with delivery scheme indicator 660 specifies the URL of a content repository. Content item indicator 666 specifies a pathname for digital content located at access domain 662 and for which access is requested and controlled by the token 664. Token indicator 664 specifies a token to use to access digital content within a context associated with the token. In this case, the context associated with the token comprises content item 666 located at access domain 662. The token 664 specifies a collection of digital content items made accessible by the token 664. Additional non-token information from content item 666 is required to completely specify the digital content accessed, thus providing relatively coarse-grained access control with respect to the URL illustrated in FIG. 6D. Presenting token 664 entitles the presenter access to digital content 666 at access domain 662.

[0058] Figure 6F is a diagram that illustrates a tokenized URL for use in accessing digital content at a particular directory or content locker of a content repository having an access domain dedicated to accepting tokenized URLs in accordance with one embodiment of the present invention. Access domain indicator 672 in combination with delivery scheme indicator

670 specifies the URL of a content repository. Content locker indicator 676 specifies the pathname of a container for at least one digital content item. Content item indicator 678 specifies a pathname for digital content located within content locker 676 at access domain 672 for which access is requested and controlled by the token 674. Token indicator 674 specifies a token to use to access digital content within a context associated with the token. In this case, the context associated with the token comprises content item 678 within content locker 676 located at access domain 672. The token specifies a collection of digital content items made accessible by the token. Additional non-token information from content locker indicator 676 and content item 678 are required to completely specify the digital content accessed, thus providing relatively coarse-grained access control with respect to the URLs illustrated in FIGS. 6D and 6E. Presenting token 674 entitles the presenter access to digital content 678 within content locker 676 at access domain 672.

[0059] In the context of the present invention, the term "servlet" comprises a program that resides and executes on a server to provide functionality to the server or processing of data on the server. By way of example, a servlet may comprise a CGI (Common Gateway Interface) script or program, ASP (Active Server Pages), a Java™ Servlet, or the like. Java™ Servlet technology is described in "Java™ Servlet Specification", version 2.3, September 17, 2001, available from Sun Microsystems, Santa Clara, CA. According to embodiments of the present invention, a specialized servlet is specified in an authenticated digital content request such as a URL. The specialized servlet handles the provisioning of digital content protected by authenticated digital content requests.

[0060] Figures 7A-7C are similar to FIGS. 6D-6F, respectively, except that the URLs in FIGS. 7A-7C additionally specify the pathname of a servlet (704, 714, 734) to process an authenticated digital content request.

[0061] Figures 8-11 illustrate various apparatus for digital content access control in accordance with embodiments of the present invention. Figure 8 illustrates a system for controlling access to program code modules such as MIDlets or the like. A MIDlet is an application that conforms to the MIDP (Mobile Information Device Profile) standard (Mobile Information Device Profile (JSR-37), JCP Specification, Java 2 Platform, Micro Edition, 1.0a, available from Sun Microsystems, Santa Clara CA). Figure 9 illustrates a system for controlling access to audio files such as MP3 files or the like. Figure 10 illustrates a system for controlling access to XML (Extensible Markup Language) documents. Figure 11 illustrates a system for controlling access to Web pages.

[0062] According to embodiments of the present invention, user devices illustrated in FIGS. 8-11 (reference numeral 800 of FIG. 8, reference numeral 900 of FIG. 9, reference numeral 1000 of FIG. 10 and reference numeral 1100 of FIG. 11) comprise a CDMA technology-enabled smart card, a SIM card, a WIM, a USIM, a UIM, a R-UIM or the like.

[0063] Figures 8-11 are intended for purposes of illustration and are not intended to be limiting in any way. Those of ordinary skill in the art will recognize the invention may be applied to any digital content regardless of digital content format or intended use.

[0064] Figures 12-14 illustrate systems for digital content access control having alternative configurations. A user device is not shown in FIGS. 12-14 and a content producer is not shown in FIGS 12-15 to avoid obfuscation of the present invention.

[0065] Turning now to FIG. 12, a block diagram that illustrates a system for digital content access control having one or more content repositories associated with a content provisioner in accordance with one embodiment of the present invention is presented. System 1200 comprises a content provisioner 1205 in communication with one or more content repositories (1210, 1215) via network 1240. Content repositories 1210 and 1215 comprise token acceptors 1225 and 1220, respectively. Content provisioner 1205 comprises a token issuer 1230 and a synchronizer 1235. Synchronizer 1235 maintains consistency in token pool information used by token issuer 1235 and token acceptors 1225 and 1220.

[0066] Turning now to FIG. 13, a block diagram that illustrates a system for digital content access control having one or more content provisioners associated with a content repository in accordance with one embodiment of the present invention is presented. System 1300 comprises a content repository 1315 in communication with one or more content provisioners (1305, 1310) via network 1340. Content provisioners 1305 and 1310 comprise token issuers 1320 and 1325, respectively. Content repository 1315 comprises a token acceptor 1330 and a synchronizer 1335. Synchronizer 1335 maintains consistency in token pool information used by token acceptor 1330 and token issuers 1305 and 1310.

[0067] Turning now to FIG. 14, a block diagram that illustrates a system for digital content access control having one or more content provisioners and content repositories associated with a synchronizer in accordance with one embodiment of the present invention is presented. System 1400 comprises one or more content provisioners (1405, 1410), one or more content repositories (1420, 1425) and a synchronizer 1415 in communication via network 1450. Content provisioners 1405 and 1410 comprise token issuers 1430 and 1435, respectively. Content repositories 1420 and 1425 comprise token acceptors 1440 and 1445, respectively. Synchronizer 1415 maintains consistency in token pool information used by token issuers 1430 and 1435, token acceptors 1440 and 1445 and synchronizer 1415. Synchronizer 1415 may be operated by a trusted third party such as a financial services provider or bank.

[0068] Turning now to FIG. 15, a block diagram that illustrates a system for digital content access control where a secure user device activates deactivated tokens issued by a content provisioner and uses the activated tokens to access digital content stored by a content repository in accordance with one embodiment of the present invention is presented. System 1500 comprises a content provisioner 1505, a content repository 1515, a user device 1565 and a synchronizer 1520 in communication via network 1560. Content provisioner 1505 comprises a token issuer 1535 and content repository 1515 comprises a token acceptor 1540. User device 1565 comprises storage for deactivated tokens (1570). User device 1565 also comprises a secure user device 1505 that comprises a co-issuer 1525. The co-issuer 1525 comprises a secret 1530 for activating deactivated tokens.

[0069] In operation, user device 1565 communicates with content provisioner 1505 to obtain one or more deactivated tokens and stores them in deactivated token storage 1570. The one or more deactivated tokens 1545 are tied to particular digital content. Co-issuer 1525 activates the one or more deactivated tokens 1545 based at least in part on secret 1530. Secure user device 1505 presents one or more activated tokens 1550 to content repository 1515 to receive access to the digital content associated with the one or more activated tokens 1550. Content repository 1515 presents synchronizer 1555 with accepted tokens 1555. The synchronizer 1520 may recycle the previously accepted tokens 1555 to make them available for future token allocations. Synchronizer 1520 may also facilitate payment for delivery of digital content and receive payment in return for the accepted tokens. Synchronizer 1520 presents tokens to be recycled 1575 to content provisioner 1505 for subsequent reuse.

[0070] According to one embodiment of the present invention, user device 1565 comprises a mobile phone and secure user device 1505 comprises a SIM card or the like.

[0071] According to one embodiment of the present invention, co-issuer 1525 activates one or more deactivated tokens 1545 upon receipt by secure user device 1505 and stores the activated tokens in secure user device 1505 until the activated tokens are redeemed for access to digital content associated with the tokens. According to another embodiment of the present invention, secure user device 1505 stores one or more deactivated tokens until access to digital content associated with the deactivated tokens is desired. At that point, co-issuer 1525 activates the deactivated tokens and presents the activated tokens 1550 to content repository 1515 for access to digital content associated with the activated tokens.

[0072] Turning now to FIG. 16, a block diagram that illustrates a system for digital content access control where a secure user device activates deactivated tokens issued by a content provisioner and uses the activated tokens to access digital content stored by a content repository in accordance with one embodiment of the present invention is presented. Figure 16 is similar to FIG. 15 except that secure user device 1605 in FIG. 16 comprises deactivated token storage 1670. In operation, user device 1665 communicates with content provisioner 1605 to obtain one or more deactivated tokens and stores them in deactivated token storage 1670. The one or more deactivated tokens 1645 are tied to particular digital content. Co-issuer 1625 activates the one or more deactivated tokens 1645 based at least in part on secret 1630. Secure user device 1605 presents one or more activated tokens 1650 to content repository 1615 to receive access to the digital content associated with the one or more activated tokens 1650. Content repository 1615 presents synchronizer 1620 with accepted tokens 1655. The synchronizer 1620 may recycle the previously accepted tokens 1655 to make them available for future token allocations. Synchronizer 1620 may also facilitate payment for delivery of digital content and receive payment in return for the accepted tokens. Synchronizer 1620 presents tokens to be recycled 1675 to content provisioner 1605 for subsequent reuse.

[0073] Turning now to FIG. 17, a block diagram that illustrates token pool allocation and synchronization in a system for digital content access control in accordance with one embodiment of the present invention is presented. According to embodiments of the present invention, a collection of one or more tokens tied to or associated with particular digital content is referred to as a token pool. A token issuer 1705 is associated with one or more issuer token

pools 1720. The token issuer 1705 accounts for issued and available tokens. A token acceptor 1710 is associated with one or more acceptor token pools 1725. The token acceptor 1710 accounts for unredeemed tokens and tokens that have been partially and fully redeemed for access to digital content associated with the token pool 1725. A token is fully redeemed if it has been redeemed a predetermined number of times. A token is not fully redeemed if it has been redeemed less than the predetermined number of times. A token is partially redeemed if it has been redeemed a number of times that is greater than zero but less than the predetermined number of times. Issuer token pool 1720 and acceptor token pool 1725 are associated with the same digital content. Synchronizer 1715 synchronizes the token pool information for issuer token pool 1720 and acceptor token pool 1725. When issuer 1705 needs to provision tokens for digital content that the issuer 1705 does not currently manage, issuer 1705 issues a new pool request 1740. Synchronizer receives the request 1740 and provides the issuer 1710 and the acceptor 1710 with at least one new token pool 1745 associated with the new digital content.

[0074] Still referring to FIG. 17, issuer 1705 or acceptor 1710 may request additional tokens when a requirement for more is determined. The issuer may make this determination based at least in part on factors such as the number of unissued tokens remaining in a particular issuer token pool or the amount of time since new tokens were received, by way of example. The acceptor may determine that more tokens are required based at least in part on factors such the number of unredeemed and partially redeemed tokens remaining in a particular acceptor token pool or the amount of time since new tokens were received, by way of example. The synchronizer 1715 may also determine that more tokens are required based at least in part on factors such as the amount of time since a token pool was replenished. When a requirement for

more tokens is determined, synchronizer 1715 provides issuer 1705 and acceptor 1710 with one or more additional tokens.

[0075] Still referring to FIG. 17, various transport mechanisms may be used to communicate information such as token pool information between the synchronizer 1715, issuer 1705 and acceptor 1710 entities. The transport mechanism may be based at least in part on the level of trust between the entities. If there is a relatively high level of trust between the entities, synchronizer 1715 may provide issuer 1705 and acceptor 1710 with the tokens for a token pool. If there is a relatively low level of trust between the entities, synchronizer 1715 may provide issuer 1705 and acceptor 1710 with a cryptogram or sealed message that comprises tokens or information for use in generating the tokens.

[0076] According to another embodiment of the present invention, token pool information is communicated from a content provisioner to a content repository using SSL (Secure Sockets Layer) or the like. Those of ordinary skill in the art will recognize that token pool information may be communicated securely from a content provisioner to a content repository using other mechanisms.

[0077] Figures 18A-18F illustrate tokens in accordance with embodiments of the present invention. A token may comprise a cryptogram as illustrated in FIG. 18A. Cryptogram 1800 may be based at least in part on the digital content associated with the token, or on a reference to the digital content. In other words, cryptogram 1800 may authenticate the protected digital content or a reference to the protected digital content. In FIG. 18B, the token comprises a

cryptogram 1810 and a chain ID 1805. Chain ID 1805 may be used to associate the token with a token pool or token chain within a token pool. According to one embodiment of the present invention, Chain ID 1805 is based at least in part on a token chain key. According to another embodiment of the present invention, chain ID 1805 comprises a pool ID and chain ID corresponding to a token chain within the token pool associated with the pool ID. In FIG. 18C, the token comprises a cryptogram 1825, a chain ID 1815 and a maximum chain length 1820. In FIG. 18D, the token comprises a cryptogram 1840, a chain ID 1830 and an offset or identifier in a series 1835. Offset 1835 may be used to identify the position within a token pool or token chain where the cryptogram 1840 is located. In other words, offset 1835 may be used to identify the location of a cryptogram 1840 in a token pool or token chain. In FIG. 18E, the token comprises a cryptogram 1855, a chain ID 1845 and an offset representing an identifier in a series 1850. In FIG. 18F, the token comprises a cryptogram 1870 and a token type indicator 1860. Token type indicator 1860 specifies the format of the token (i.e. what to expect in token fields 1865 and 1870). Reference numeral 1865 represents one or more token fields. By way of example, reference numeral 1865 may comprise one or more of the fields illustrated in FIGS. 18A-18E, and token type indicator 1860 may specify the format of token fields 1865 and 1870 .

[0078] The token formats illustrated in FIGS. 18A-18F are for purposes of illustration and are not intended to be limiting in any way. A token may also comprise an Extensible Markup Language (XML)-formatted Hypertext Markup Language (HTML)-encoded message with fields as illustrated in FIGS. 18A-18E. Additionally, a cryptogram may comprise other fields and other combinations of fields illustrated in FIGS. 18A-18F.

[0079] According to embodiments of the present invention, a token pool comprises one or more token chains that comprise one or more tokens. Figures 19, 20 and 21 illustrate creating tokens for subsequent use in creating a tokenized URL. Figure 19 illustrates creating a token chain by applying a cryptographic process to one or more identifiers in a series together with a token chain key, FIG. 20 illustrates creating a token chain by applying a cryptographic process to a filler and one or more identifiers in a series together with a token chain key, and FIG. 21 illustrates creating a token chain using cryptographic one-way functions.

[0080] Turning now to FIG. 19, a block diagram that illustrates creating a token chain by applying a cryptographic process to one or more identifiers in a series together with a token chain key with in accordance with one embodiment of the present invention is presented. Token chain 1944 comprises a plurality of tokens 1930-1938. Seed 1904 may be based at least in part on a portion of a URL, where the URL defines digital content that may be accessed using a token from a token pool based at least in part on the seed 1904. According to one embodiment of the present invention, a cryptographic process (1906) is applied to seed 1904 to create a token chain key 1908. According to one embodiment of the present invention, the cryptographic process (1906) comprises a hashing function. According to another embodiment of the present invention, the token chain key 1908 is created by applying a cryptographic process (1906) to the seed 1904 together with a token pool key 1900. According to another embodiment of the present invention, the token chain key 1908 is created by applying a cryptographic process (1906) to the seed 1904 and the maximum length of the token chain 1902. Tokens 1930-1938 are created by applying a cryptographic process to (1910-1918) identifiers 1920-1928, respectively, together with the token chain key 1908.

[0081] Turning now to FIG. 20, a block diagram that illustrates creating a token chain by applying a cryptographic process to a filler and one or more identifiers in a series together with a token chain key in accordance with one embodiment of the present invention is presented. Tokens 2030-2038 are created by replacing a predefined set of bits of a filler 2046 with the one or more bits expressing an identifier in a series (2020-2028) and applying a cryptographic process (2010-2018) to the modified filler 2046 together with the token chain key 2008. According to one embodiment of the present invention, tokens are allocated in order of token creation. Tokens may be pre-generated. Alternatively, the last identifier used to generate a token is stored and this stored value is used to generate tokens one-at-a-time as needed.

[0082] Turning now to FIG. 21, a block diagram that illustrates creating a token chain using cryptographic one-way functions in accordance with one embodiment of the present invention is presented. Token chain key 2100 is used to create the first token 2140 and tokens 2145-2155 are based at least in part on tokens 2140-2150, respectively. Token 2160 is based at least in part on the token that precedes it (the token corresponding to position M (2185) minus one). According to one embodiment of the present invention, the token allocation order is the reverse of the token generation order. Using FIG. 21 as an example, the last-generated token 2160 is also the first-allocated token. Similarly, the first-generated token 2140 is also the last-allocated token.

[0083] According to one embodiment of the present invention, the first token 2140 is created by applying a cryptographic process (2115) to a length value 2105 that indicates the number of tokens in the corresponding token chain 2102, together with a token chain key 2100. According

to one embodiment of the present invention, the cryptographic process (2115) comprises a hashing function. According to another embodiment of the present invention, the first token 2140 is created by applying a cryptographic process (2115) to the token chain key 2100 together with a token pool key 2110 that is shared by token chains within a token pool. According to another embodiment of the present invention, the first token 2140 is created by applying a cryptographic process (2115) to a length value 2105 and the token chain key 2100 together with a token pool key 2110.

[0084] The data used to create the first token 2140 determines how token validation is performed. By way of example, length value 2105 may be fixed for a particular token pool and known to both token issuer and token acceptor. In this case, both the issuer and the acceptor may generate tokens in a token chain associated with token chain key 2100 independent of whether a synchronizer provides a length value with a token chain key 2100. However, if the length field 2105 is not known to both issuer and token acceptor and if the length value is used to create the first token 2140, a synchronizer may provide the length value 2105 with the associated token chain key 2100. Alternatively, a token may comprise a length value as illustrated above with respect to reference numeral 1820 of FIG. 18.

[0085] Turning now to FIG. 22, a flow diagram that illustrates a method for creating and using a token pool formed by applying a cryptographic process to an identifier in a series together with a token chain key in accordance with one embodiment of the present invention is presented. Figure 22 corresponds to FIG. 19. At 2200, a token pool that comprises a token chain where each token in a token chain is formed by applying a cryptographic process to one or more

bits expressing an identifier in a series together with a token chain key is created. At 2205, the tokens in the token chain are allocated based on authenticated user requests for one or more resources associated with the token pool. According to one embodiment of the present invention, token allocation is ordered according to the token creation order such that the first-allocated token comprises the first-created token and the last-allocated token comprises the last-created token. According to another embodiment of the present invention, a randomized process is used to select an unallocated token within the token chain.

[0086] The process corresponding to FIG. 20 is similar to the flow diagram illustrated in FIG. 22, except that at reference numeral 2200, each token in a token chain is formed by replacing a predefined set of bits of a filler with the one or more bits expressing an identifier in a series and applying a cryptographic process to the modified filler together with a token chain key.

[0087] Turning now to FIG. 23, a flow diagram that illustrates a method for creating and using a token pool formed by successive applications of a cryptographic one-way function in accordance with one embodiment of the present invention is presented. Figure 23 corresponds to FIG. 21. At 2300, a token pool that comprises a token chain where each token in a token chain is formed by applying a cryptographic one-way function to the token immediately preceding the current token in the token chain is created. At 2305, the tokens in the token chain are allocated in reverse sequential order based on authenticated user requests for one or more resources associated with the token pool, beginning with the last-created token in the token chain.

[0088] As mentioned with reference to FIG. 17, a synchronizer communicates token validation information to a content repository that allows the content repository to validate received tokens. The token validation information may comprise one or more token pools or information used to generate the pools. The synchronizer may transfer the token validation information using a secure protocol such as SSL or the like. Alternatively, the synchronizer may transfer encrypted token validation information. This encrypted token validation information may also be transferred using a further secure protocol such as SSL or the like.

[0089] According to one embodiment of the present invention, the token validation information transferred by a synchronizer comprises a token pool. In response to a token synchronization event (such as when a requesting entity requests an additional token pool), a synchronizer generates a token pool comprising tokens and sends the tokens to the requesting entity and optionally to one or more non-requesting entities. The requesting entity and the non-requesting entities may comprise a content repository or a content provisioner. If the requesting entity is a content repository, content repository receives the token pool and uses it to validate authenticated digital content requests. If the requesting entity is a content provisioner, the content provisioner receives the token pool and uses it to generate authenticated digital content requests.

[0090] According to another embodiment of the present invention, a token comprises a chain ID as illustrated in FIGS. 18B-18E. In this case, the synchronizer transfers token pool keys. Upon receiving an authenticated digital content request, the content repository uses the chain ID of the received token to determine which token chain to check. If the content repository is

configured to pre-compute token pools, the token chain associated with the received chain ID is checked for the cryptogram associated with the received token. If the content repository is not configured to pre-compute token pools, the chain ID is used in the computation to check the cryptogram associated with the received token, which comprises generating all or part of the token chain. Upon the occurrence of a synchronization event, such as when the amount of tokens available for redemption falls below a predetermined threshold, the synchronizer sends one or more token pool keys.

[0091] Figure 24 illustrates transferring one or more token chain keys and possibly additional information from a synchronizer. A cryptographic process 2426 is applied to a portion (2420, 2422, 2424) of a URL 2462, together with a key 2428. The URL 2462 identifies the protected digital content. According to one embodiment of the present invention, the URL comprises a content domain indicator (2420). According to another embodiment of the present invention, the URL comprises a content domain indicator and a content directory indicator (2422). According to another embodiment of the present invention, the URL comprises a content domain indicator, a content directory indicator and a content item indicator (2424). The cryptographic process may additionally be applied to a randomized number 2466 or a chain length 2435. According to one embodiment of the present invention, the cryptographic process comprises encryption. According to another embodiment of the present invention, the cryptographic process comprises a hashing function. The result of the cryptographic process is a token chain key 2430. The token chain key 2430 is encrypted with a transport key 2436, creating sealed token pool information 2438. A chain length, a portion of a URL 2462, or both may also be encrypted at 2432.

[0092] Still referring to FIG. 24, the decision regarding whether to encrypt the chain length or the URL at 2432 may be based on factors such as a level of trust with the receiving entity, and whether cryptographic process 2426 is reversible. If cryptographic process 2426 is irreversible and if the receiving entity requires additional information such as the chain length and the URL, the additional information is included in the data encrypted at 2432. The sealed token pool information 2438 may be communicated to a content provisioner for use in issuing authenticated digital content requests. The sealed token pool information may also be communicated to a content repository for use in validating authenticated digital content requests.

[0093] According to one embodiment of the present invention, cryptographic process 2426 corresponds to cryptographic process 1906 in FIG. 19. According to another embodiment of the present invention, cryptographic process 2426 corresponds to cryptographic process 2006 in FIG. 20. According to one embodiment of the present invention, cryptographic process 2426 corresponds to cryptographic process 2115 in FIG. 21. Those of ordinary skill in the art will recognize that other cryptographic processes may be used.

[0094] Still referring to FIG. 24, at 2440 a receiving entity such as a content repository or a content provisioner receives the sealed token pool information 2438 and decrypts it using a transport key 2442 agreed with the synchronizer. The contents of the unsealed token pool information depend upon what was input to the encryption process at 2432. As shown in FIG. 24, the unsealed token pool information comprises a token chain key 2446, a chain length 2444 and a portion of a URL 2448. A token generation process 2454 uses the unsealed token pool information to generate a token pool 2452. If the receiving entity is a content provisioner, the

tokens in the token pool are used to create authenticated digital content requests. If the receiving entity is a content repository, the tokens in the token pool are used to validate authenticated digital content requests.

[0095] The mechanisms used to communicate token pool information as shown and described with respect to FIG. 24 are for illustrative purposes only and are not intended to be limiting in any way. Other cryptographic methods and sealed data may be used.

[0096] Figures 25 and 26 illustrate token pools comprising one or more token chains that comprise one or more tokens in accordance with embodiments of the present invention. Figure 25 illustrates a single token pool that comprises one or more token chains created using cryptographic one-way functions, and FIG. 26 illustrates a single token pool that comprises one or more smaller token pools that may be organized as described with respect to FIG. 25.

[0097] As mentioned above, the term "cryptographic one-way function" describes any cryptographic process that produces an output based upon an input, such that it is computationally infeasible to compute the input based upon the output. However, it is less difficult to compute a later-generated token when an earlier-generated token is known. Therefore, it may be possible to receive an earlier-generated token and compute a later-generated token that has been issued but has not been redeemed. This computed token may then be used to obtain unauthorized access to digital content and consequently prevent the authorized recipient of the token from using the token to obtain access to digital content. According to one embodiment of the present invention, a token pool comprises one or more token chains created

using cryptographic one-way functions. Tokens are issued from alternating chains, decreasing the per-token-chain number of tokens that have been issued but have not been redeemed, and thus decreasing the likelihood that a valid but unauthorized token may be computed based upon a previously generated token. This is explained in more detail below with reference to FIG. 25.

[0098] Turning now to FIG. 25, a block diagram that illustrates allocating tokens from a token pool comprising one or more token chains created using a cryptographic one-way function in accordance with one embodiment of the present invention is presented. Token pool 2500 comprises token chains 2504-2528. Token chains 2504-2528 comprise a predetermined number of tokens. According to one embodiment of the present invention, a token in a token chain is formed by applying a cryptographic one-way function to the previous token as illustrated with respect to FIGS. 21 and 23.

[0099] According to one embodiment of the present invention, tokens in a token pool as illustrated in FIG. 25 are allocated with each successive token allocation originating from a token chain that is different than the last. Where tokens in a token pool are based upon encrypting a number in a series as illustrated with respect to FIGS. 19, 20 and 22, a randomized selection process may be used to select an unallocated token from a particular token chain.

[0100] According to another embodiment of the present invention, tokens in a token pool as illustrated in FIG. 25 are allocated beginning with the last-generated token 2530 in the first token chain 2504 and continuing in a diagonal pattern. Cryptographic one-way functions are used to create the tokens in the token chains. Since the per-chain token allocation order is the reverse of

the token generation order, allocation of the first-generated token indicates the token chain has been fully allocated. Accordingly, one or more additional token chains are requested upon allocating the first-generated token in what is currently the last token chain. This obviates the need for a more complex mechanism for determining whether another token chain should be requested, such as counting the number of tokens allocated and requesting an additional chain at predetermined intervals.

[0101] Figure 25 shows the state of token pool 2500 after several tokens have been allocated. As shown in FIG. 25, all tokens in token chain 2504 have been allocated, token chains 2506-2522 are partially allocated and token chains 2524-2528 are unallocated. Diagonal 2532 indicates the last-allocated tokens and diagonal 2534 indicates the tokens to be allocated next, beginning with token 2536 and ending with token 2538. According to one embodiment of the present invention, a determination regarding whether to request additional token chains is made upon allocating the last token in a token chain. Using FIG. 25 as an example, the previous determination regarding whether to request additional token chains was made upon allocating token 2538, the current determination is made upon allocating token 2536 and the next determination will be made upon allocating token 2538. The determination may be based at least in part on one or more factors such as the number of tokens per chain and the token allocation rate.

[0102] The number of token chains and the number of tokens in each token chain as shown in FIG. 25 are not intended to be limiting in any way. Those of ordinary skill in the art will recognize that the number of tokens in each token chain and the number of token chains in a

token pool may vary. Additionally, the number of tokens in each token chain need not be uniform with respect to one or more token chains within a token pool.

[0103] According to embodiments of the present invention, a token pool comprises a plurality of smaller token pools. This is described below in detail with reference to FIG. 26.

[0104] Turning now to FIG. 26, a block diagram that illustrates a token pool having a current token pool for current token redemptions, a retired token pool for tokens that have been available for redemption for a predetermined time and a buffered token pool for future token redemptions in accordance with one embodiment of the present invention is presented. In operation, a content repository satisfies token redemption requests from a current token pool 2615 and a retired token pool 2610. An indication is made when a token is redeemed so that a token is redeemed a predetermined number of times. According to one embodiment of the present invention, this predetermined number of times is one. When the decision is made to start satisfying token redemption requests from a new token pool, the retired token pool 2610 is discarded, the current token pool 2615 becomes the retired token pool 2610, the buffered token pool 2605 becomes the current token pool 2615 and a new buffered token pool 2605 is received.

[0105] According to one embodiment of the present invention, the decision to start satisfying token redemption requests from a new token pool is based at least in part on the number of unredeemed tokens remaining in the current token pool 2615. By way of example, a content repository may be configured such that redemption requests begin to be satisfied from a new

token pool when the number of tokens not fully redeemed remaining in the current token pool falls below ten.

[0106] According to another embodiment of the present invention, the decision to start satisfying token redemption requests from a new token pool is based at least in part on the amount of time that the current token pool has been available for satisfying token redemption requests. By way of example, a content repository may be configured such that redemption requests begin to be satisfied from a new token chain when a current token chain has been available for satisfying token redemption requests for ten or more minutes.

[0107] According to another embodiment of the present invention, the decision to start satisfying token redemption requests from a new token pool is based at least in part on instructions provided by an external source, such as a content provisioner. By way of example, a content repository may be configured begin satisfying token redemption requests from a new token pool when instructed to do so by a digital content provisioner.

[0108] Figures 27-33 illustrate initialization of a system for digital content access control in accordance with embodiments of the present invention. Figures 34-51 illustrate operation of a system for digital content access control in accordance with embodiments of the present invention.

[0109] Turning now to FIG. 27, a detailed block diagram that illustrates initialization of a system for digital content access control in accordance with one embodiment of the present

invention is presented. System 2746 comprises at least one user device 2700, at least one content provisioner 2734, at least one content repository 2708 and at least one content producer 2710 that communicate via network 2706. User device 2700 is configured to send a digital content request and receive digital content in response to the digital content request. User device 2700 may be any device configured to render digital content to a user 2702.

[0110] According to embodiments of the present invention, user device 2700 comprises a CDMA technology-enabled smart card, a SIM card, a WIM, a USIM, a UIM, a R-UIM or the like.

[0111] Content provisioner 2724 is configured to receive a digital content request and return an authenticated digital content request in response to the received digital content request. Content provisioner 2724 comprises a provisioner manager 2704, a content rights database 2714 and a content catalog 2722. Content rights database 2714 is configured to store an association between one or more users 2702 and a description of the digital content that the one or more users are authorized to access. Content catalog 2722 comprises a description of digital content stored by one or more digital content repositories 2708.

[0112] Still referring to FIG. 27, provisioner manager 2704 comprises a token issuer 2720, a download manager 2716, a content descriptor loader 2718 and a synchronizer 2730. Content descriptor loader 2718 is configured to load one or more content descriptors provided by one or more content producers 2710. Download manager 2716 is configured to receive a digital content request such as a portion of a URL or the like and communicate with content rights database

2722 to determine whether the user is authorized to access the digital content. Download manager 2716 is also configured to send a token request if access is authorized, receive the requested token and create an authenticated digital content request based at least in part on the token and the digital content request. Synchronizer 2730 is configured to synchronize token information between content provisioner 2724 and content repository 2708. According to one embodiment of the present invention, an authenticated digital content request comprises a tokenized URL.

[0113] Still referring to FIG. 27, download manager 2716 is also configured to send the authenticated digital content request. Token issuer 2720 is configured to receive a token request, generate a token associated with the digital content for which access is requested, and return the token.

[0114] Content repository 2708 is configured to receive an authenticated digital content request and return digital content corresponding to the authenticated digital content request. Content repository 2708 comprises a repository manager 2744 and a database 2738. Database 2738 comprises digital content 2740 and a token pool 2742 associated with the digital content 2740.

[0115] Still referring to FIG. 27, repository manager 2744 comprises a token acceptor 2734. Token acceptor 2734 is configured to accept digital content request information. The authenticated digital content request information may comprise, by way of example, a token pool, information for use in generating a token pool, and the number of tokens released by the

content provisioner. The information may also comprise one or more token chain keys and corresponding token chain lengths. Token acceptor 2734 is also configured to accept a token and communicate with token pool 2742 to determine whether the token is valid for the digital content requested.

[0116] Content producer 2710 is configured to provide digital content to content repository 2708. Content producer 2710 is also configured to provide at least one digital content description corresponding to the digital content stored by at least one content repository 2708.

[0117] During initialization of system 2746, at least one content producer 2710 provides digital content to at least one content repository 2708. Content repository 2708 stores the digital content in database 2738. Content producer 2710 also provides a description of the same content to at least one content provisioner 2724. Content descriptor loader 2718 receives the content description and sends it to content catalog 2722 in content provisioner 2724.

[0118] Turning now to FIG. 28, a flow diagram that illustrates a method for digital content access control from the perspective of a user device in accordance with one embodiment of the present invention is presented. At 2800, a user device is received. At 2805, a user uses the user device to enroll with a content provisioner. During the enrollment process, the user authenticates himself or herself to the content provisioner and may provide payment information such as authorization to charge a credit card or authorization to debit a debit card or checking account for digital content made accessible by tokens issued to the user.

[0119] Turning now to FIG. 29, a flow diagram that illustrates a method for digital content access control from the perspective of a secure user device in accordance with one embodiment of the present invention is presented. Figure 29 corresponds with FIGS. 15 and 16. At 2900, a user device is received. At 2905, the user uses the user device to enroll with a content provisioner. At 2910, the secret is stored for use in activating tokens on a secure user device.

[0120] According to another embodiment of the present invention, enrolling with a content provisioner (2805, 2905) and receiving a secure user device (2800, 2900) is combined into one cryptographic process, such that a user receives a secure user device enabled to receive digital content upon successfully enrolling with the content provisioner.

[0121] Turning now to FIG. 30, a flow diagram that illustrates a method for initializing a digital content producer in accordance with one embodiment of the present invention is presented. At 3000, digital content is produced. By way of example, a digital music producer creates digital files (such as MP3 files) that store musical content. At 3005, the content producer provides the digital content to a content repository. At 3010, the content producer provides a description of the digital content to a content provisioner. Using the above example, the digital content producer provides musical content such as digital musical tracks to the content repository. The content producer also provides a description of the digital content (such as the artist and title of the musical tracks) to a content provisioner.

[0122] According to another embodiment of the present invention, a content producer provides digital content and a description of the digital content to a synchronizer. The

synchronizer generates token pool information associated with the digital content, sends the digital content and token pool information to a content repository and sends the digital content description and token pool information to a content provisioner.

[0123] Turning now to FIG. 31, a flow diagram that illustrates a method for initializing a digital content provisioner in accordance with one embodiment of the present invention is presented. At 3100, a token pool message is received from a synchronizer. The message may be encrypted. At 3105, token pool information is extracted from the pool message. At 3110, the token issuer is initialized with token pool information from the token pool message.

[0124] Turning now to FIG. 32, a flow diagram that illustrates a method for content repository initialization in accordance with one embodiment of the present invention is presented. At 3200, digital content from a content provider is received. At 3208, a token pool message from a synchronizer is received. The message may be encrypted. At 3210, token pool information is extracted from the token pool message. At 3215, a token acceptor is initialized with the token pool information from the token pool message.

[0125] Turning now to FIG. 33, a flow diagram that illustrates a method for synchronizer initialization in accordance with one embodiment of the present invention is presented. At 3300, a description of the digital content to be protected is received. The description may comprise, by way of example, a URL, part of a URL, a summary of the digital content, a hash of the digital content, or the like. At 3300, token pool information is generated. At 3305, the token pool

information is sent to one or more content provisioners. At 3310, the token pool information is sent to one or more content repositories.

[0126] Turning now to FIG. 34, a detailed block diagram that illustrates a system for digital content access control in accordance with one embodiment of the present invention is presented. Figure 34 illustrates using tokens to access digital content once the system has been initialized as described with respect to FIGS. 27-33. In operation, user device 3400 sends a digital content request in the form of a URL to content provisioner 3404 via portal 3458. Download manager 3414 in provisioner manager 3424 receives the URL and communicates with content rights database 3422 to verify whether the user 3402 is authorized to access the digital content associated with the URL. If the user 3402 is authorized to access the digital content associated with the URL, download manager 3414 sends a token request 3444 to token issuer 3420. Token issuer 3420 receives the token request 3444 and communicates with content catalog 3418 to obtain a token associated with the digital content referenced by the URL. Token issuer 3420 sends the token 3446 to download manager 3414. Download manager creates a tokenized URL 3448 based at least in part on the URL 3440 and the token 3446 and sends the tokenized URL 3448 to user device 3400 via portal 3458. User device 3400 sends the tokenized URL 3450 to content repository 3408 via network 3406. Token acceptor 3432 in repository manager 3456 receives the tokenized URL 3450 and communicates with token pool 3440 in database 3436 to determine whether the tokenized URL 3450 is valid. If the tokenized URL 3450 is valid, the digital content associated with the tokenized URL 3450 is obtained from digital content storage 3438 and sent to user device 3400 via network 3406.

[0127] Turning now to FIG. 35, a flow diagram that illustrates a method for digital content access control from the perspective of a user device in accordance with one embodiment of the present invention is presented. Figure 35 illustrates operation of a user device in a system such as system 370 in FIG. 3, where a content provisioner does not communicate directly with a content repository to obtain digital content associated with a digital content request. At 3500, a digital content request is sent to a content provisioner capable of authenticating the request. At 3505, an authenticated digital content request is received in response to sending the digital content request. At 3510, the authenticated digital content request is sent to a content repository that provides storage for the digital content. At 3515, digital content corresponding to the authenticated digital content request is received in response to the authenticated digital content request.

[0128] As mentioned above with respect to FIG. 4, according to one embodiment of the present invention, a requesting user device issues a digital content request and a receiving user device receives digital content in response to the digital content request. In more detail with reference to FIG. 35, the requesting user device (reference numeral 400 of FIG. 4) sends a digital content request (3500) to a content provisioner, receives an authenticated digital content request (3505) and sends the authenticated digital content request to a content repository that provides storage for the digital content (3510). The authenticated digital content request may comprise delivery information, or may be used to obtain delivery information. The delivery information may indicate a receiving device that is different from the requesting device. The receiving user device (reference numeral 402 of FIG. 4) receives digital content corresponding to the digital content request (3515).

[0129] Turning now to FIG. 36, a flow diagram that illustrates a method for digital content access control from the perspective of a user device in accordance with one embodiment of the present invention is presented. Figure 36 illustrates operation of a user device in a system such as system 598 in FIG. 5, where a portal handles communication between a content provisioner and a content repository to obtain digital content associated with a digital content request entered by a user. According to one embodiment of the present invention, the portal that handles communications between a user device and a content provisioner also handles communications between the content provisioner and the content repository. At 3600, a digital content request is sent to a content provisioner capable of authenticating the request. At 3605, digital content corresponding to the digital content is received in response to the digital content request.

[0130] Turning now to FIG. 37, a flow diagram that illustrates a method for digital content access control from the perspective of a secure user device in accordance with one embodiment of the present invention is presented. Figure 37 corresponds with FIGS. 15 and 16. At 3700, a deactivated token for accessing digital content is received. At 3705, the deactivated token is activated using a secret stored on the secure user device. At 3710, an authenticated digital content request is created based at least in part on the activated token. At 3715, the authenticated digital content request is sent to a content repository that provides storage for the digital content. At 3720, digital content corresponding to the digital content request is received.

[0131] Turning now to FIG. 38, a flow diagram that illustrates a method for digital content access control from the perspective of a digital content provisioner in accordance with one

embodiment of the present invention is presented. At 3800, a request for access to digital content is received. At 3805, a determination is made regarding whether the user that issued the request is authorized to access the digital content. The result of this determination is checked at 3810. If the requested access is unauthorized, an exception is indicated at 3815. If the requested access is authorized, an authenticated digital content request is created at 3820 and at 3825, the authenticated digital content request is sent for use in accessing the digital content from a content repository. At 3830, a determination is made regarding whether pool synchronization is enabled. Pool synchronization comprises determining whether additional tokens are required and requesting additional tokens if it is determined that more are required. If enabled, pool synchronization is performed at 3835.

[0132] Turning now to FIG. 39, a flow diagram that illustrates a method for digital content access control from the perspective of a digital content provisioner in accordance with one embodiment of the present invention is presented. Figure 39 corresponds with FIGS. 15 and 16. At 3900, a request for access to digital content is received. At 3905, a determination is made regarding whether the user that issued the request is authorized to access the digital content. The result of this determination is checked at 3910. If the requested access is unauthorized, an exception is indicated at 3915. If the requested access is authorized, at 3920 a deactivated token is sent for use in accessing digital content stored by a content repository. At 3925, a determination is made regarding whether pool synchronization is enabled. If enabled, pool synchronization is performed at 3930.

[0133] Turning now to FIG. 40, a flow diagram that illustrates a method for creating an authenticated digital content request in accordance with one embodiment of the present invention is presented. Figure 40 provides more detail for reference numeral 3820 of FIG. 38. At 4000, the token pool associated with the particular digital content is determined. At 4005, an unallocated token in the token pool is determined. At 4010, a tokenized URL is created based at least in part on the token.

[0134] Turning now to FIG. 41, a flow diagram that illustrates a method for digital content access control from the perspective of a digital content repository in accordance with one embodiment of the present invention is presented. At 4100, an authenticated digital content request is received. At 4105, the authenticated digital content request is validated. At 4110, a determination is made regarding whether the authenticated digital content request is valid. If the authenticated digital content request is invalid, an exception is indicated at 4115. If the authenticated digital content request is valid, a determination is made regarding whether pool synchronization is enabled at 4120. If enabled, pool synchronization is performed at 4125. At 4130, the digital content associated with the digital content request is provided.

[0135] Figures 42-50 illustrate validating an authenticated digital content request in accordance with embodiments of the present invention. Figures 42-50 provide more detail for reference numeral 4105 of FIG. 41. Figure 42 illustrates validating an authenticated digital content request using a pre-computed token pool comprising multi-use tokens. Figures 43-47 illustrate validating an authenticated digital content request by dynamically computing tokens using a sliding token offset window. Figure 48 illustrates validating an authenticated digital

content request using a pre-computed token pool comprising single-use tokens computed using a cryptographic one-way function. Figure 49 illustrates validating an authenticated digital content request using a pre-computed token pool comprising single-use tokens computed using a cryptographic one-way function and ordered according to token redemption status. Figure 50 illustrates validating an authenticated digital content request by dynamically computing single-use tokens using a cryptographic one-way function. These validation methods are explained in more detail below.

[0136] Turning now to FIG. 42, a flow diagram that illustrates a method for validating an authenticated digital content request using a pre-computed token pool comprising multi-use tokens in accordance with one embodiment of the present invention is presented. At 4200, a token is received. At 4205, a determination is made regarding whether there are any unredeemed or partially redeemed tokens left in the token pool. If there is at least one unredeemed or partially redeemed token remaining in the token pool, at 4210 a determination is made regarding whether the received token is in the token pool. If the received token is in the token pool, at 4215 a determination is made regarding whether the received token has been fully redeemed. If the received token is fully redeemed at 4215, or if the received token is not in the token pool at 4210, or if there are no unredeemed tokens left to check at 4205, at 4230 an indication that the received token is invalid is made. If at 4215 the received token has not been fully redeemed, a token redemption count associated with the received token is incremented at 4220, and an indication that the received token is valid is made at 4225.

[0137] Figures 43-46 illustrate using a sliding token offset window for dynamic token computation in accordance with one embodiment of the present invention. Figure 43 depicts a sliding token offset window, and FIG. 44 illustrates a method for using a sliding token offset window. Figure 45 illustrates a method for validating an authenticated digital content request by dynamically computing tokens using a sliding token offset window having a dynamic size. Figure 46 illustrates a method for validating an authenticated digital content request by dynamically computing tokens using a sliding token offset window having a static size.

[0138] According to embodiments of the present invention, a window management policy determines the criteria for moving the bottom of the window and the top of the window. The window may be moved as part of a token synchronization process. The window may also be moved as part of a token validation process.

[0139] According to embodiments of the present invention, the criteria for moving the bottom or top of a window may be based at least in part on the amount of time since the window was last moved.

[0140] Turning now to FIG. 43, a block diagram that illustrates a sliding token offset window for use in dynamic token computation in accordance with one embodiment of the present invention is presented. As shown in FIG. 43, data structure 4300 comprises a list of offset entries 4302-4334. Sliding window 4334 comprises a predetermined number of offset entries. Offset entries within window 4334 are identified by a base number 4336 and an offset 4338 from the base number. The offsets for entries 4324, 4322, 4320, 4318, 4316, 4314, 4312

and 4310 are 0-7, respectively. According to one embodiment of the present invention, the ordinal number of an identifier in a series comprises the sum of an offset 4338 and a base number 4336. Similarly, the offset 4338 comprises the ordinal number of the identifier in a series, minus the base number 4336.

[0141] Still referring to FIG. 43, an offset entry is associated with an offset redemption status. According to one embodiment of the present invention, a token may be redeemed a predetermined number of times. In this case, the possible offset redemption status values comprise an "unredeemed" status, a "partially redeemed" status and a "fully redeemed" status. According to another embodiment of the present invention, a token may be redeemed once. In this case, the possible token redemption status values comprise a "fully redeemed" status and a "not fully redeemed" status. An offset is fully redeemed if a token based at least in part on the offset has been redeemed a predetermined number of times. An offset is not fully redeemed if a token based at least in part on the offset has been redeemed less than the predetermined number of times. An offset is partially redeemed if a token based at least in part on the offset has been redeemed a number of times that is greater than zero but less than the predetermined number of times.

[0142] According to embodiments of the present invention, data structure 4300 is used to determine whether a received token has been fully redeemed. The determination comprises summing the base number 4336 and an offset within sliding window 4334, where the offset has an offset redemption status of "unredeemed" or "partially redeemed". The sum is used as an input to a cryptographic process that computes a token. If the result of the cryptographic process

matches the received token, a valid token is indicated and the offset redemption status of the offset is updated to account for the redemption. This process is explained in more detail below with reference to FIG. 44.

[0143] Turning now to FIG. 44, a flow diagram that illustrates a method for validating an authenticated digital content request by dynamically computing tokens using a sliding token offset window in accordance with one embodiment of the present invention is presented. At 4400, a token is received. At 4405, a determination is made regarding whether there are any unredeemed or partially redeemed offsets within an offset window. If there is at least one unredeemed or partially redeemed offset within the offset window, at 4410 an offset within the window that has not been fully redeemed is selected. At 4415, a cryptographic process is applied to the sum of the base number and the selected offset. At 4420, a determination is made regarding whether the result of the cryptographic process matches the received token. If there is no match, another offset is selected beginning at 4405. If there is a match, the offset redemption status of the selected offset is updated at 4425 to account for the redemption and at 4430, an indication that the received token is valid is made. If none of the results of applying the cryptographic process to the sum of the base number and each unredeemed or partially redeemed offsets match the received token, an indication that the received token is invalid is made at 4435.

[0144] Figures 45 and 46 are similar to FIG. 44, except that the received token in FIGS. 45 and 46 comprises token offset information, as illustrated above with respect to FIGS. 18D and 18E. Additionally, the windows in FIGS. 45 and 46 are modified when the offset is above the

token window. In FIG. 45, the window is expanded upwards to include the offset. In FIG. 46, the window is moved upwards to include the offset.

[0145] Turning now to FIG. 45, a flow diagram that illustrates a method for validating an authenticated digital content request by dynamically computing tokens using a sliding token offset window having a dynamic size in accordance with one embodiment of the present invention is presented. At 4500, a token comprising token offset information is received. At 4505, a determination is made regarding whether the offset is within a token offset window. If the offset is not within the token offset window, at 4510 a determination is made regarding whether the offset is above the window. If the token is not above the window, an indication that the token is invalid is made at 4540. If the offset is above the window, at 4515 the window is expanded upwards to include the offset. At 4520, a cryptographic process is applied to the sum of the base number and the offset. At 4525, a determination is made regarding whether the result of the cryptographic process matches the received token. If there is no match, an indication that the token is invalid is made at 4540. If there is a match, at 4545 a determination is made regarding whether the token is fully redeemed. If the token is fully redeemed, an indication that the token is invalid is made at 4540. If the token is not fully redeemed, the offset redemption status of the offset is updated at 4530 to account for the redemption and at 4535, an indication that the received token is valid is made.

[0146] Turning now to FIG. 46, a flow diagram that illustrates a method for validating an authenticated digital content request by dynamically computing tokens using a sliding token offset window having a static size in accordance with one embodiment of the present invention is

presented. Figure 46 is similar to FIG. 45, except that the window is moved upwards to include the offset (4615) when the offset is above the window in FIG. 46, whereas the window is expanded upwards to include the offset (4515) when the offset is above the window in FIG. 45.

[0147] Turning now to FIG. 47, a flow diagram that illustrates a method for updating an offset in accordance with one embodiment of the present invention is presented. Figure 47 provides more detail for reference numerals 4425, 4530 and 4630 of FIGS. 44, 45 and 46, respectively. At 4700, the redemption status of the offset is updated. At 4705, a determination is made regarding whether the offset is at the bottom of the window. If the offset is at the bottom of the window, the window is moved upwards. According to one embodiment of the present invention, the window is moved up one position. According to another embodiment of the present invention, the window is moved up until the bottom of the window comprises an unredeemed or partially redeemed offset.

[0148] Turning now to FIG. 48, a flow diagram that illustrates a method for validating an authenticated digital content request using a pre-computed token pool comprising single-use tokens computed using a cryptographic one-way function in accordance with one embodiment of the present invention is presented. At 4800, a token is received. At 4805, a determination is made regarding whether there are any unredeemed tokens left in the token pool. If there is at least one unredeemed token remaining in the token pool, at 4810 a determination is made regarding whether the received token is in the token pool. If the received token is in the token pool, at 4815 a determination is made regarding whether the token has been redeemed. If the token has not been redeemed, at 4820 an indication is made that the token is valid. At 4825,

tokens in the token chain that were generated after the received token are invalidated. If there are no tokens left to check at 4805, or if the received token is not in the token pool at 4810, or if the received token has been redeemed (4815), an indication that the token is invalid is made at 4830.

[0149] Turning now to FIG. 49, a flow diagram that illustrates a method for validating an authenticated digital content request using a pre-computed token pool comprising single-use tokens computed using a cryptographic one-way function and ordered according to token redemption status in accordance with one embodiment of the present invention is presented. At 4900, a token is received. At 4905, a determination is made regarding whether there are any unredeemed tokens left in the token pool. If there is at least one unredeemed token remaining in the token pool, at 4910 a determination is made regarding whether the received token is in a portion of the token pool comprising redeemed tokens. If the received token has not been redeemed, at 4915 an indication that the received token is valid is made. At 4920, the tokens of the token pool are reordered based upon their token redemption status. If there are no tokens left to check at 4905, or if the token has been redeemed (4910), an indication that the token is in valid is made at 4925.

[0150] Turning now to FIG. 50, a flow diagram that illustrates a method for validating an authenticated digital content request by dynamically computing single-use tokens using a cryptographic one-way function in accordance with one embodiment of the present invention is presented. At 5000, a token is received. At 5005, the current token is set to the received token. At 5010, a determination is made regarding whether there are any unredeemed tokens left in a

token pool. If there is at least one unredeemed token remaining, at 5015 a determination is made regarding whether the received token matches the last redeemed token. If the received token does not match the last received token, at 5020 the current token is set to the result of applying a cryptographic one-way function to the current token. At 5025, a determination is made regarding whether the current token matches the last redeemed token. If the current token matches the last redeemed token, an indication that the token is valid is made at 5035 and the last redeemed token is set to the received token at 5040. If the current token does not match the last redeemed token at 5025, at 5030 a determination is made regarding whether there is another unredeemed token in the token pool. If there is another token in the token pool, the next token is checked beginning at 5020. If there are no more tokens in the token pool at 5030, or if the received token matches the last redeemed token at 5015, or if there are no tokens left to check at 5010, an indication that the token is invalid is made at 5045.

[0151] Figures 42, 44, 48, 49 and 50 include an initial determination regarding whether there are any tokens or offsets left to be checked (reference numerals 4205, 4405, 4805, 4905 and 5010, respectively). This determination may comprise checking a variable comprising this token information. Alternatively, the determination may comprise searching for one or more tokens or offsets that have not been fully redeemed.

[0152] Turning now to FIG. 51, a flow diagram that illustrates a method for digital content access control from the perspective of a synchronizer in accordance with one embodiment of the present invention is presented. At 5100, a determination is made regarding whether a synchronization event has been received. According to one embodiment of the present

invention, a synchronization event comprises the receipt of a synchronization request. According to another embodiment of the present invention, a synchronization event is generated at predetermined intervals. If a synchronization event has been received, at 5105 token pool information is determined. At 5110, a determination is made regarding whether the synchronization event is an internal event. A synchronization event is an internal event if it is triggered by the synchronizer. An exemplary internal event is a synchronization event triggered by the synchronizer at a predetermined interval. A synchronization event is an external event if it is triggered by an entity other than the synchronizer. If the synchronization event is an internal event, at 5115 token pool information is sent to all entities that need to know the information. If the synchronization event is not an internal event, at 5120 the token pool information is sent to a possible requesting party. The requesting party may be, by way of example, a content provisioner or a content repository. At 5125, a determination is made regarding whether the token pool information should be sent to a non-requesting party. If the token pool information should be sent to the non-requesting party, it is done at 5130.

[0153] According to one another embodiment of the present invention, token pool information determined in response to a synchronization request is sent to the requesting party. By way of example, upon receiving a synchronization request from a content provisioner, the synchronizer sends token pool information to the content provisioner.

[0154] According to another embodiment of the present invention, token pool information determined in response to a synchronization request is sent to both the requesting party and one or more non-requesting parties regardless of the identity of the requesting party. By way of

example, upon receiving a synchronization request from a content provisioner, the synchronizer sends token pool information to both the content provisioner and a content repository.

[0155] Figures 52-57B illustrate mechanisms for controlled delivery of digital content to a target device in a system for digital content access control in accordance with embodiments of the present invention. The embodiments illustrated in FIGs. 52-57B enable low-level control of digital content delivered to target devices, while requiring relatively little overhead for encryption. Delivery parameters determined by a content provisioner or user device specify a target device to receive requested digital content. The target device includes a target key that is unique to the particular target device and is used to decrypt digital content that has been encrypted for limited time use by that particular target device. Figures 52-53 illustrate controlled delivery of digital content to a target device via a user device. Figures 54-55 illustrate controlled delivery of digital content to a user device that is also a target device. Figures 56A-57B provide more detail for the encryption and decryption methods used in the embodiments illustrated in FIGs. 52-55.

[0156] Turning now to FIG. 52, a block diagram that illustrates controlled delivery of digital content to a target device via a user device in a system for digital content access control in accordance with one embodiment of the present invention is presented. System 5270 may comprise at least one user device 5200, at least one content provisioner 5252 and at least one content repository 5282 that communicate via a network 5210. System 5270 may also comprise a synchronizer 5262 in communication with the content provisioner 5252 and the content repository 5282. User device 5200 is configured to send a digital content request 5250 to at least

one content provisioner 5275, and receive an authenticated digital content request such as a tokenized URL 5255 in response to the digital content request 5250. The tokenized URL 5255 includes one or more delivery parameters comprising a target ID. User device 5200 is also configured to send the tokenized URL including the target ID to at least one content repository 5290 and receive encrypted digital content in response to the tokenized URL. User device 5200 is also configured to send the token of the tokenized URL and the encrypted digital content to target device 5202. User device 5200 may also be configured to send one or more delivery parameters to target device 5202.

[0157] In the context of the present invention, a target ID identifies one or more target devices to receive requested digital content. A target ID may uniquely identify a single target device. Alternatively, a target ID may identify a group of target devices. A target ID may comprise a serial number of one or more target devices, a textual description of one or more target devices, or an alias for one or more target devices.

[0158] In the context of the present invention, the term "delivery parameter" describes an identifier that identifies one or more of the following: a destination or target for receipt of requested digital content, a decryption algorithm identifier for use in identifying a decryption algorithm to employ in decrypting encrypted digital content (5265, 5254, 5275) sent to one or more target devices 5202, a master key 5280 for use in decrypting encrypted digital content (5265, 5254, 5275), a key derivation process supported by one or more target devices 5202, and a cryptographic process supported by one or more target devices 5202. A target device 5202 may use a specified key derivation process to derive or determine a cryptographic key for use in

decrypting encrypted digital content (5265, 5254, 5275). A target device 5202 may use a specified cryptographic process to decrypt encrypted digital content (5265, 5254, 5275).

[0159] Still referring to FIG. 52, target device 5202 is configured to receive a token and encrypted digital content 5254 from user device 5200. Target device 5202 may be any device configured to render digital content to a user 5205. By way of example, target device 5202 may comprise a personal digital assistant (PDA), a personal computer (PC), a mobile phone, a digital audio player (such as an MP3 player), a game console, a server computer in communication with a user display, or the like. According to another embodiment of the present invention, target device 5202 comprises a secure portable device such as a Java Card™ technology-enabled device, or the like.

[0160] According to embodiments of the present invention, target device 5202 comprises a CDMA technology-enabled smart card, a SIM card, a WIM, a USIM, a UIM, a R-UIM or the like.

[0161] Referring again to FIG. 52, content provisioner 5252 is configured to receive a digital content request 5250 and return an authenticated digital content request such as a tokenized URL including one or more delivery parameters 5255 in response to the received digital content request 5250. Content provisioner 5252 may comprise a content rights database 5215 to store an association between one or more users and a description of the digital content that the one or more users are authorized to access. The description may comprise one or more target IDs associated with a user, and a description of the digital content that may be delivered to one or

more target devices corresponding to the target IDs. The description may also comprise one or more delivery parameter conditions that specify one or more required characteristics of parameter values associated with a parameter. By way of example, delivery parameter conditions may specify a quality of service associated with delivery of the digital content to target devices corresponding to the target IDs. Furthermore, the required characteristics may be specified with varying levels of particularity. A characteristic specified with a relatively high level of particularity includes, by way of example, a requirement that a specific cryptographic key, a cryptographic algorithm, or both, be used in cryptographically protecting digital content sent to target devices. A characteristic specified with a relatively low level of particularity includes, by way of example, a requirement that a cryptographic key comprising a predetermined number of bits be used to protect digital content sent to target devices.

[0162] Still referring to FIG. 52, content provisioner 5252 may also comprise a provisioner manager 5275 in communication with the content rights database 5215. The provisioner manager 5275 is configured to receive a digital content request 5250 and communicate with content rights database 5215 to determine whether the user 5205 that made the request 5250 is authorized to access the digital content associated with the request 5250. The provisioner manager 5275 may comprise an issuer 5276 to issue a token for use in creating an authenticated digital content request 5255. Alternatively, content provisioner 5252 may comprise an issuer external to and in communication with a provisioner manager. The provisioner manager 5275 is also configured to communicate with user device 5200 to obtain user authentication data such as a password, PIN, biometric data or the like. If the user device 5200 comprises a mobile phone, the user authentication data may also comprise a mobile phone subscriber ID, or the like.

According to one embodiment of the present invention, the authenticated digital content request 5255 comprises a cryptogram based at least in part on an identifier that describes the location of the digital content for which access is authorized. According to another embodiment of the present invention, the cryptogram comprises at least one token from a token pool associated with the location of the digital content for which access is authorized.

[0163] Content repository 5282 is configured to receive an authenticated digital content request 5260 and return encrypted digital content corresponding to the authenticated digital content request 5260. According to one embodiment of the present invention, the encrypted digital content 5265 is returned to the user device 5200 that issued the authenticated digital content request 5260. According to another embodiment of the present invention, the encrypted digital content 5275 is delivered to at least one target device 5202 corresponding to a target ID specified by the one or more delivery parameters comprising a target ID.

[0164] Content repository 5282 may comprise a content database 5290 to store digital content corresponding to at least one digital content description stored by at least one content provisioner 5252. Content repository 5282 also may comprise a repository manager 5266 in communication with the content database 5290. The repository manager 5266 is configured to receive an authenticated digital content request 5260, communicate with the content database 5290 to determine whether the authenticated digital content request 5260 is valid, and return the digital content associated with the authenticated digital content request 5260 when the authenticated digital content request 5260 is valid. The repository manager 5266 may also comprise an acceptor 5264 to accept a token and determine whether the access to the digital

content associated with the authenticated digital content request is authorized based at least in part on the token. Alternatively, content repository 5282 may comprise an acceptor external to and in communication with a repository manager 5266.

[0165] Synchronizer 5262 is configured to synchronize the information used by the content provisioner 5252 to create authenticated digital content requests with the information used by content repository 5282 to validate digital content requests. The authenticated digital content request information may comprise, by way of example, a token pool, information for use in generating a token pool, or the number of tokens released by the content provisioner 5252. According to one embodiment of the present invention, the content provisioner 5252 triggers the synchronization. According to another embodiment of the present invention, the content repository 5282 triggers the synchronization. According to another embodiment of the present invention, the synchronization is triggered by the synchronizer 5262, based at least in part on a predetermined schedule.

[0166] In operation, user device 5200 sends a digital content request 5250 to content provisioner 5252. According to one embodiment of the present invention, the digital content request 5250 is based at least in part on information received from content provisioner 5252. This information may comprise, by way of example, an indication of one or more services available to user 5205. Provisioner manager 5275 in content provisioner 5252 receives the digital content request 5250 and communicates with content rights database 5215 to determine whether the user 5205 that made the request 5250 is authorized to access the digital content associated with the request 5250. Provisioner manager 5275 may also communicate with user

device 5200 to obtain user authentication data such as a password, PIN, biometric data or the like. If the user device 5200 comprises a mobile phone, the user authentication data may also comprise a mobile phone subscriber ID, or the like. If the user 5205 that made the request 5250 is authorized to access the digital content 5238 associated with the digital content request 5250, issuer 5275 issues a token and provisioner manager 5275 creates an authenticated digital content request 355 based at least in part on the token. The content provisioner also determines one or more delivery parameters.

[0167] User device 5200 receives the authenticated digital content request 355 and then sends the authenticated digital content request 5260 to a content repository 5282. Repository manager 5266 in content repository 5282 receives the authenticated digital content request 5282 and communicates with acceptor 5264 and content database 5290 to determine whether the authenticated digital content request 5260 is valid. If the authenticated digital content request 5260 is valid, repository manager 5266 applies a cryptographic process to the master key, the token key, the target ID, and possibly one or more delivery parameters or other indications to create a session key. The cryptographic process may comprise encryption. Alternatively, the cryptographic process may comprise keyed hashing. Other cryptographic processes may be used. The repository manager 5266 then encrypts the digital content with the session key and returns the encrypted digital content 5238 associated with the authenticated digital content request 5260. According to one embodiment of the present invention, the encrypted digital content 5265 is returned to the user device 5200 that issued the authenticated digital content request 5260. According to another embodiment of the present invention, the encrypted digital

content 5275 is delivered to a target device 5202 corresponding to a target ID specified by the one or more delivery parameters.

[0168] Upon receiving the encrypted digital content 5265, user device 5200 sends the encrypted digital content 5254, the token 5256 of the tokenized URL, and one or more delivery parameters to target device 5202. Upon receiving the encrypted digital content 5254, the token 5256, and the one or more delivery parameters, target device 5202 uses target key 5295 and a token key based at least in part on the token 5256 in a cryptographic process to create a session key. The cryptographic process may comprise encryption. Alternatively, the cryptographic process may comprise keyed hashing. Other cryptographic processes may be used. The session key is used to decrypt the encrypted digital content 5254 to obtain digital content 5238 for rendering to user 5205.

[0169] Turning now to FIG. 53, a flow diagram that illustrates controlled delivery of digital content to a target device via a user device in a system for digital content access control in accordance with one embodiment of the present invention is presented. Figure 53 corresponds with FIG. 52. At 5330, a content provisioner 5304 receives a digital content request 5350. At 5332, an authenticated digital content request such as a tokenized URL is created. At 5334, one or more delivery parameters are optionally determined. At 5336, the authenticated digital content request and one or more delivery parameters 5318 are sent to the user device 5300 that issued the digital content request.

[0170] At 5308, the user device 5300 receives the authenticated digital content request and one or more delivery parameters 5318. At 5352, one or more delivery parameters are optionally determined. At 5310, the authenticated digital content request and one or more delivery parameters 5320 are sent to a content repository 5306. As mentioned above, a content provisioner 5304 may determine one or more delivery parameters. According to another embodiment of the present invention, the one or more delivery parameters are determined by the user device 5300 before sending (5310) the authenticated digital content request and one or more delivery parameters to the content repository 5306. At 5312, one or more delivery parameters and the token in a tokenized URL or other authenticated digital content request is sent to the target device 5302 specified by the one or more delivery parameters.

[0171] At 5340, the content repository 5306 receives the authenticated digital content request and one or more delivery parameters 5318 sent by the user device 5300. At 5342, a session key is determined. At 5344, digital content to be sent is located. At 5346, the digital content is encrypted using the session key. At 5348, the encrypted digital content is sent. According to one embodiment of the present invention, the encrypted digital content 5338 is sent to the user device that sent the tokenized URL. According to another embodiment of the present invention, the encrypted digital content 5350 is sent to the target device 5302.

[0172] Still referring to FIG. 53, at 5314 the user device 5300 receives encrypted digital content 5338 sent by the content repository 5306. At 5316, the encrypted digital content 5338 is sent to the target device 5302 specified by the one or more delivery parameters.

[0173] At 5322, the target device 5302 receives the token and one or more delivery parameters sent at 5312. At 5324, a token key based at least in part on the token is used in a cryptographic process to create a session key. The cryptographic process may comprise encryption. Alternatively, the cryptographic process may comprise keyed hashing. Other cryptographic processes may be used. At 5326, the encrypted digital content received directly (5350) from the content repository 5306 or indirectly via the user device 5300 is decrypted using the session key. At 5328, the digital content is rendered. By way of example, if the digital content comprises a digital audio file (such as an MP3 file), the digital audio file may be rendered by generating an audible communication representing the contents of the digital audio file.

[0174] Turning now to FIG. 54, a block diagram that illustrates controlled delivery of digital content to a target device in a system for digital content access control in accordance with one embodiment of the present invention is presented. Figure 54 is similar to FIG. 52 except that in FIG. 54, a user device is identified by a target ID. System 5470 may comprise at least one target device 5400, at least one content provisioner 5452 and at least one content repository 5482 that communicate via a network 5410. System 5470 may also comprise a synchronizer 5462 in communication with the content provisioner 5452 and the content repository 5482. Target device 5400 is configured to send a digital content request 5450 to at least one content provisioner 5452, and receive an authenticated digital content request such as a tokenized URL 5455 in response to the digital content request 5450. The tokenized URL 5455 includes one or more delivery parameters.

[0175] Still referring to FIG. 54, target device 5400 is also configured to send the tokenized URL including the target ID to at least one content repository 5482 and receive encrypted digital content in response to the tokenized URL. Target device 5400 may be any device configured to render digital content to a user 5405. By way of example, target device 5400 may comprise a personal digital assistant (PDA), a personal computer (PC), a mobile phone, a digital audio player (such as an MP3 player), a game console, a server computer in communication with a user display, or the like. According to another embodiment of the present invention, target device 5400 comprises a secure portable device such as a Java Card™ technology-enabled device, or the like.

[0176] According to embodiments of the present invention, target device 5400 comprises a CDMA technology-enabled smart card, a SIM card, a WIM, a USIM, a UIM, a R-UIM or the like.

[0177] Referring again to FIG. 54, content provisioner 5452 is configured to receive a digital content request 5450 and return an authenticated digital content request such as a tokenized URL including one or more delivery parameters 5455 in response to the received digital content request 5450. Content provisioner 5452 may comprise a content rights database 5415 to store an association between one or more users and a description of the digital content that the one or more users are authorized to access. The description may comprise one or more target IDs associated with a user, and a description of the digital content that may be delivered to target devices corresponding to the target IDs. The description may also comprise one or more delivery parameter conditions that specify one or more required characteristics of parameter

values associated with a parameter. By way of example, delivery parameter conditions may specify a quality of service associated with delivery of the digital content to target devices corresponding to the target IDs. Furthermore, the required characteristics may be specified with varying levels of particularity. A characteristic specified with a relatively high level of particularity includes, by way of example, a requirement that a specific cryptographic key, a cryptographic algorithm, or both, be used in cryptographically protecting digital content sent to target devices. A characteristic specified with a relatively low level of particularity includes, by way of example, a requirement that a cryptographic key comprising a predetermined number of bits be used to protect digital content sent to target devices.

[0178] Still referring to FIG. 54, content provisioner 5452 may also comprise a provisioner manager 5475 in communication with the content rights database 5415. The provisioner manager 5475 is configured to receive a digital content request 5450 and communicate with content rights database 5415 to determine whether the user 5405 that made the request 5450 is authorized to access the digital content associated with the request 5450. The provisioner manager 5475 may comprise an issuer 5476 to issue a token for use in creating an authenticated digital content request 5455. Alternatively, content provisioner 5452 may comprise an issuer external to and in communication with a provisioner manager. The provisioner manager 5475 is also configured to communicate with target device 5400 to obtain user authentication data such as a password, PIN, biometric data or the like. If the target device 5400 comprises a mobile phone, the user authentication data may also comprise a mobile phone subscriber ID, or the like. According to one embodiment of the present invention, the authenticated digital content request 5455 comprises a cryptogram based at least in part on an identifier that describes the location of

the digital content for which access is authorized. According to another embodiment of the present invention, the cryptogram comprises at least one token from a token pool associated with the location of the digital content for which access is authorized.

[0179] Content repository 5482 is configured to receive an authenticated digital content request 5460 and return encrypted digital content 5465 corresponding to the authenticated digital content request 5460. According to one embodiment of the present invention, the encrypted digital content 5465 is returned to the user device 5400 that issued the authenticated digital content request 5460. The user device 5400 is identified by a target ID specified by the one or more delivery parameters.

[0180] Content repository 5482 may comprise a content database 5490 to store digital content corresponding to at least one digital content description stored by at least one content provisioner 5452. Content repository 5482 also may comprise a repository manager 5466 in communication with the content database 5490. The repository manager 5466 is configured to receive an authenticated digital content request 5460, communicate with the content database 5490 to determine whether the authenticated digital content request 5460 is valid, and return the digital content associated with the authenticated digital content request 5460 when the authenticated digital content request 5460 is valid. The repository manager 5466 may also comprise an acceptor 5464 to accept a token and determine whether the access to the digital content associated with the authenticated digital content request 5460 is authorized based at least in part on the token. Alternatively, content repository 5482 may comprise an acceptor external to and in communication with a repository manager 5466.

[0181] Synchronizer 5462 is configured to synchronize the information used by the content provisioner 5452 to create authenticated digital content requests with the information used by content repository 5482 to validate digital content requests. The authenticated digital content request information may comprise, by way of example, a token pool, information for use in generating a token pool, and the number of tokens released by the content provisioner 5452. According to one embodiment of the present invention, the content provisioner 5452 triggers the synchronization. According to another embodiment of the present invention, the content repository 5482 triggers the synchronization. According to another embodiment of the present invention, the synchronization is triggered by the synchronizer 5462, based at least in part on a predetermined schedule.

[0182] In operation, target device 5400 sends a digital content request 5450 to content provisioner 5452. According to one embodiment of the present invention, the digital content request 5450 is based at least in part on information received from content provisioner 5452. This information may comprise, by way of example, an indication of one or more services available to user 5405. Provisioner manager 5475 in content provisioner 5452 receives the digital content request 5450 and communicates with content rights database 5415 to determine whether the user 5405 that made the request 5450 is authorized to access the digital content associated with the request 5450. Provisioner manager 5475 may also communicate with target device 5400 to obtain user authentication data such as a password, PIN, biometric data or the like. If the target device 5400 comprises a mobile phone, the user authentication data may also comprise a mobile phone subscriber ID, or the like. If the user 5405 that made the request 5450

is authorized to access the digital content 5465 associated with the digital content request 5450, issuer 5475 issues a token and provisioner manager 5475 creates an authenticated digital content request 355 based at least in part on the token. The content provisioner also determines one or more delivery parameters.

[0183] Target device 5400 receives the authenticated digital content request 355 and then sends the authenticated digital content request 5460 to a content repository 5482. Repository manager 5466 in content repository 5482 receives the authenticated digital content request 5482 and communicates with acceptor 5464 and content database 5490 to determine whether the authenticated digital content request 5460 is valid. If the authenticated digital content request 5460 is valid, repository manager 5466 applies a cryptographic process to the master key, the token key, the target ID, and possibly one or more delivery parameters or other indications to create a session key. The cryptographic process may comprise encryption. Alternatively, the cryptographic process may comprise keyed hashing. Other cryptographic processes may be used. The repository manager 5466 then encrypts the digital content with the session key, and returns the encrypted digital content 5465 associated with the authenticated digital content request 5460. According to one embodiment of the present invention, the encrypted digital content 5465 is returned to the user device 5400 that issued the authenticated digital content request 5460. The user device 5400 is identified by a target ID specified by the one or more delivery parameters.

[0184] Upon receiving the encrypted digital content 5465, target device 5400 uses target key 5495 and a token key based at least in part on the token of the tokenized URL 5455 in a

cryptographic process to create a session key. The cryptographic process may comprise encryption. Alternatively, the cryptographic process may comprise keyed hashing. Other cryptographic processes may be used. The session key is used to decrypt the encrypted digital content 5465 to obtain digital content 5438 for rendering to user 5405.

[0185] According to embodiments of the present invention, target devices illustrated in FIGs. 52 and 54 (reference numeral 5202 of FIG. 52 and reference numeral 5400 of FIG. 54) comprise a CDMA technology-enabled smart card, a SIM card, a WIM, a USIM, a UIM, a R-UIM or the like.

[0186] Turning now to FIG. 55, a flow diagram that illustrates controlled delivery of digital content to a target device in a system for digital content access control in accordance with one embodiment of the present invention is presented. Figure 55 corresponds with FIG. 54. At 5518, a content provisioner 5502 receives a digital content request 5516. At 5520, an authenticated digital content request such as a tokenized URL is created. At 5522, one or more delivery parameters are optionally determined. At 5524, the authenticated digital content request and one or more delivery parameters are sent to the user device 5500 that issued the digital content request.

[0187] At 5506, the user device 5500 receives the authenticated digital content request and one or more delivery parameters 5526. At 5552, one or more delivery parameters are optionally determined. At 5508, the authenticated digital content request and one or more delivery parameters 5528 are sent to a content repository 5504. As mentioned above, a content

provisioner 5502 may determine one or more delivery parameters. According to another embodiment of the present invention, the one or more delivery parameters are determined by the user device 5500 before sending (5508) the authenticated digital content request and one or more delivery parameters to the content repository 5504.

[0188] At 5532, the content repository 5504 receives the authenticated digital content request and one or more delivery parameters 5528 sent by the user device 5500. At 5534, a session key is determined. At 5536, digital content to be sent is located. At 5538, the digital content is encrypted using the session key. At 5540, the encrypted digital content is sent to the user device that sent the tokenized URL.

[0189] Still referring to FIG. 55, at 5510 a token key based at least in part on the token of the tokenized URL is used in a cryptographic process to create a session key. The cryptographic process may comprise encryption. Alternatively, the cryptographic process may comprise keyed hashing. Other cryptographic processes may be used. At 5512, the user device 5500 receives encrypted digital content 5530 sent by the content repository 5504. At 5512, the encrypted digital content received from the user device 5300 is decrypted using the session key. At 5514, the digital content is rendered. By way of example, if the digital content comprises a digital audio file (such as an MP3 file), the digital audio file may be rendered by generating an audible communication representing the contents of the digital audio file.

[0190] Figures 56A-57B provide more detail for the preparation and use of a session key to cryptographically protect digital content in the embodiments illustrated in FIGs. 52-55. Figures

56A and 56B provide a high level illustration of encrypting and decrypting digital content for controlled delivery of digital content to a target device in a system for digital content access control. Figures 57A and 57B provide a low level illustration of encrypting and decrypting digital content for controlled delivery of digital content to a target device in a system for digital content access control.

[0191] Turning now to FIG. 56A, a high level data flow diagram that illustrates encrypting digital content for controlled delivery of digital content to a target device in a system for digital content access control in accordance with one embodiment of the present invention is presented. Figure 56A provides more detail for reference numerals 5343 and 5346 of FIG. 53, and reference numerals 5534 and 5538 of FIG. 55. At 5608, a cryptographic process is applied to a target ID 5604 together with a master key 5600 and a token key 5610 to create a session key 5612. The cryptographic process 5608 may comprise encryption. Alternatively, the cryptographic process 5608 may comprise keyed hashing. Other cryptographic processes may be used. At 5620, digital content 5616 is encrypted together with a session key 5612 to create encrypted digital content 5618.

[0192] Turning now to FIG. 56B, a high level data flow diagram that illustrates decrypting digital content for controlled delivery of digital content to a target device in a system for digital content access control in accordance with one embodiment of the present invention is presented. Figure 56B provides more detail for reference numerals 5324 and 5326 of FIG. 53, and reference numerals 5510 and 5512 of FIG. 55. At 5658, a cryptographic process is applied to a target ID 5654 together with a master key 5650 and a token key 5660 to create a session key 5662. The

cryptographic process 5658 may comprise encryption. Alternatively, the cryptographic process 5658 may comprise keyed hashing. Other cryptographic processes may be used. At 5670, encrypted digital content 5666 is decrypted using the session key 5662 to create decrypted digital content 5668.

[0193] Figures 57A-57B are low level data flow diagrams that illustrate encrypting and decrypting digital content for controlled delivery of digital content to a target device in a system for digital content access control in accordance with one embodiment of the present invention. Figures 57A and 57B are similar to FIGS. 56A and 56B, respectively, except FIGS. 57A and 57B illustrate using a target key in an intermediate cryptographic process to create the session key. The target key is created by applying a cryptographic process to the master key together with the target ID. Figures 57A-57B make clear that cryptographic process 5658 of FIG. 56B may be split into two sub processes: a first cryptographic process 5702 that uses a target ID 5704 and a master key 5700 to produce a target key 5706, and a second cryptographic process 5708 that uses the target key 5706 and a token key 5710 to produce a session key 5712. The first cryptographic process 5702 may be part of an enrollment process, where the target key 5706 is created and communicated to the enrolled target device. A key exchange protocol may be used to communicate the target key to the target device. The target key may be stored on the target device for subsequent use in creating one or more session keys. Once enrollment has taken place, the second cryptographic process 5728 may be applied to the target key 5726 stored on the target device, together with a token key 5730 to create a session key 5732 for use in cryptographically protecting digital content 5738. This is explained in more detail below, with reference to FIGS. 57A and 57B.

[0194] Turning now to FIG. 57A, a low level data flow diagram that illustrates encrypting digital content for controlled delivery of digital content to a target device in a system for digital content access control in accordance with one embodiment of the present invention is presented. Figure 57A provides more detail for reference numerals 5343 and 5346 of FIG. 53, and reference numerals 5534 and 5538 of FIG. 55. At 5702, a cryptographic process is applied to a target ID 5704 together with a master key 5700 to create a target key 5706. At 5708, a cryptographic process is applied to a token key based at least in part on a token 5710 together with the target key 5706 to create a session key 5712. Cryptographic process 5702 and 5708 may comprise encryption. Alternatively, the cryptographic process 5702 and 5708 may comprise keyed hashing. Other cryptographic processes may be used. Additionally, cryptographic process 5702 may be different than cryptographic process 5708.

[0195] At 5714, digital content 5716 to be delivered to a target device corresponding to the target ID 5704 is encrypted together with the session key 5712 to create encrypted digital content 5718. According to one embodiment of the present invention, a content repository stores target keys corresponding to target IDs of target devices authorized to receive digital content from the content repository. The stored target keys are used to create session keys upon receipt of tokenized URLs, and the session keys are used to encrypt digital content to be delivered to the corresponding target devices.

[0196] Turning now to FIG. 57B, a low level data flow diagram that illustrates decrypting digital content for controlled delivery of digital content to a target device in a system for digital

content access control in accordance with one embodiment of the present invention is presented. Figure 57B provides more detail for reference numerals 5324 and 5326 of FIG. 53, and reference numerals 5510 and 5512 of FIG. 55. At 5728, a cryptographic process is applied to a token key based at least in part on a token 5730 together with the target key 5726 to create a session key 5732. The cryptographic process 5728 may comprise encryption. Alternatively, the cryptographic process 5728 may comprise keyed hashing. Other cryptographic processes may be used. The target key 5726 is loaded and may be produced as illustrated in FIG. 57A. At 5734, encrypted digital content 5736 received from a content repository is decrypted using the session key 5732 to create digital content 5718 to be rendered by the target device corresponding to the target ID 5704. According to one embodiment of the present invention, a target device stores its target key corresponding to its target ID. The stored target key is used to create a session key upon receipt of a token from a tokenized URL, and the session key is used to decrypt digital content delivered to the target device.

[0197] While embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art having the benefit of this disclosure that many more modifications than mentioned above are possible without departing from the inventive concepts herein. The invention, therefore, is not to be restricted except in the spirit of the appended claims.